

The New York Times

BOOK OF

Mathematics



MORE THAN 100 YEARS OF
WRITING BY THE NUMBERS

Edited by

GINA KOLATA

Foreword by

PAUL HOFFMAN

Other Contributors Include

James Gleick, William L. Laurence, Malcolm W. Browne,
George Johnson, John Markoff, and Many More

The New York Times is one of the most authoritative voices in math and science. Now this comprehensive collection offers the very best math writings from the newspaper's extensive archives.

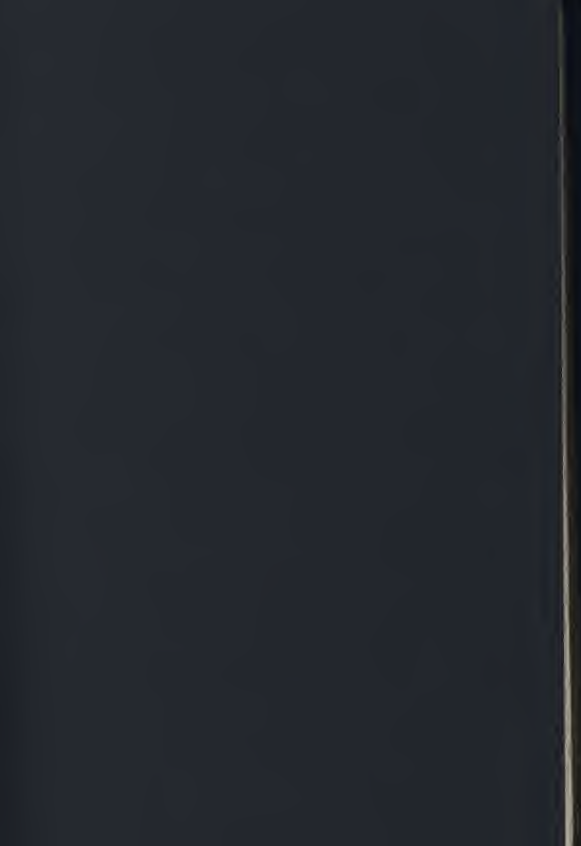
Edited by Pulitzer Prize finalist and senior *New York Times* writer Gina Kolata, this expansive, informative book gives mathematical solutions to everyday questions, reveals dramatic tales of the search for solutions to famous mathematicians' problems, sheds light on discoveries that changed the way we live and work, and paints portraits of notable mathematicians, such as the brilliant but eccentric Paul Erdős who had no home and no job. Renowned contributors include James Gleick, William L. Laurence, Malcolm W. Browne, George Johnson, and John Markoff, among others.

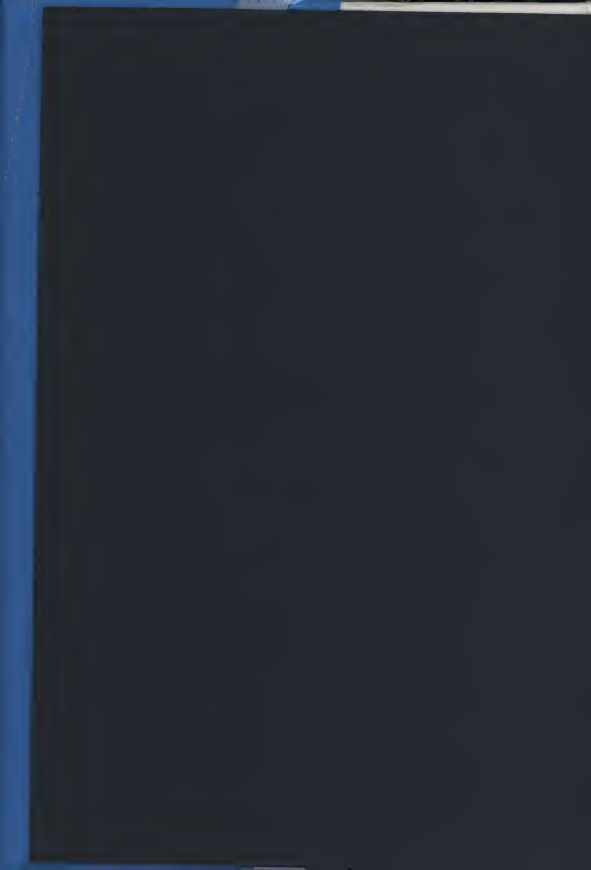
Written from the years of 1892 to 2010, these 110 articles cover everything from coincidences and randomness to cryptography and computers.

- "When Chaos Rules the Market" by James Gleick: "The economy, like complex systems in nature, combines forces on the microscopic scale and the global scale. Just as the observable behavior of the earth's atmosphere emerges from the interaction of a nearly infinite number of molecules, large-scale movements in the financial markets arise from millions of individual decisions to buy and sell."

—November 22, 1987

- "How a Gap in the Fermat Proof Was Bridged" by Gina Kolata: "Fermat's Last Theorem, which has tantalized mathematicians for more than 350 years, has at last been solved, say those who have read the revised but not yet published proof. But the endgame of this 500-year chase has proved as full of last-minute twists as a murder mystery." —January 31,





The New York Times

BOOK OF

Mathematics



The New York Times

BOOK OF

Mathematics



MORE THAN 100 YEARS OF
WRITING BY THE NUMBERS

Edited by

GINA KOLATA

Foreword by

PAUL HOFFMAN





STERLING
New York

An Imprint of Sterling Publishing
387 Park Avenue South
New York, NY 10016

STERLING and the distinctive Sterling logo are registered trademarks
of Sterling Publishing Co., Inc.

© 2013 by The New York Times Company. All rights reserved.
All Material in this book was first published in *The New York Times* and
is copyright © The New York Times Company. All rights reserved.

The printing, copying, redistribution, or retransmission of the
Material without express written permission is prohibited.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or
transmitted, in any form or by any means, electronic, mechanical, photocopying, recording,
or otherwise, without prior written permission from the publisher.

ISBN 978-1-4027-9322-6

Distributed in Canada by Sterling Publishing
c/o Canadian Manda Group, 165 Dufferin Street
Toronto, Ontario, Canada M6K 3H6

Distributed in the United Kingdom by GMC Distribution Services
Castle Place, 166 High Street, Lewes, East Sussex, England BN7 1XU

Distributed in Australia by Capricorn Link (Australia) Pty. Ltd.
P.O. Box 704, Windsor, NSW 2756, Australia

For information about custom editions, special sales, and premium and corporate purchases,
please contact Sterling Special Sales at 800-805-5489 or specialsales@sterlingpublishing.com.

Manufactured in the United States of America

2 4 6 8 10 9 7 5 3 1

www.sterlingpublishing.com

CONTENTS

Foreword <i>Paul Hoffman</i>	x
Introduction <i>Gina Kolata</i>	xiii

CHAPTER 1

What Is Mathematics?

Useful Invention or Absolute Truth: What Is Math? <i>George Johnson</i>	3
But Aren't Truth and Beauty Supposed to be Enough? <i>James Gleick</i>	9
Mathematicians Meet Computerized Ideas <i>Gina Kolata</i>	13
Mathematicians Finally Log On <i>James Gleick</i>	16
With Major Math Proof, Brute Computers Show Flash of Reasoning Power <i>Gina Kolata</i>	19
Computers Still Can't Do Beautiful Mathematics <i>Gina Kolata</i>	24
100 Quadrillion Calculations Later, Eureka! <i>Gina Kolata</i>	27
Theorist Applies Computer Power to Uncertainty in Statistics <i>Gina Kolata</i>	29

CHAPTER 2

Statistics, Coincidences and Surprising Facts

1-in-a-Trillion Coincidence, You Say? Not Really, Experts Find <i>Gina Kolata</i> ...	35
Sometimes Heavier Objects Go to the Top: Here's Why <i>James Gleick</i>	40
Behind Monty Hall's Doors: Puzzle, Debate and Answer? <i>John Tierney</i>	43
What If They Closed 42d Street and Nobody Noticed? <i>Gina Kolata</i>	48
Down for the Count; Why Some Numbers Are Only Very Good Guesses <i>Gina Kolata</i>	51
Could It Be? Weather Has Nothing to Do with Your Arthritis Pain? <i>Gina Kolata</i>	54
Electronics to Aid Weather Figuring <i>Sidney Shalett</i>	58
Insurance as a Study; Something of the Men Who Figure Business by Algebra	62
Leontief's Contribution <i>Leonard Silk</i>	64
Many Small Events May Add Up to One Mass Extinction <i>Malcolm W. Browne</i>	67
Metric Mania <i>John Allen Paulos</i>	70
In Shuffling Cards, 7 Is a Winning Number <i>Gina Kolata</i>	73

Can Game Theory Predict When Iran Will Get the Bomb? <i>Clive Thompson</i> . . .	77
In Modeling Risk, the Human Factor Was Left Out <i>Steve Lohr</i>	88
Playing the Odds <i>George Johnson</i>	92
Monday Puzzle: Solution to Birthday Problem <i>Pradeep Mutalik</i>	95
Just What Are Your Odds in Genetic Roulette? Go Figure <i>Gina Kolata</i>	102
The 2000 Election: The Science of Counting <i>Gina Kolata</i>	106
Prospectus; Can a Computer Program Figure Out the Market? A Former Analyst and a Mathematician Are Betting That Theirs Can <i>Janet Stites</i> . .	107
New Tools for the I.R.S. to Sniff Out Tax Cheats <i>David Cay Johnston</i>	110

CHAPTER 3

Famous Problems, Solved and As Yet Unsolved

New Mathematics Links Two Worlds <i>William L. Laurence</i>	115
An Elusive Proof and Its Elusive Prover <i>Dennis Overbye</i>	119
Ask Science: Poincaré's Conjecture <i>Dennis Overbye</i>	125
Grigori Perelman's Beautiful Mind <i>Jascha Hoffman</i>	131
A Math Problem Solver Declines a \$1 Million Prize <i>Dennis Overbye</i>	133
"Four-Color Problem" Attacked <i>William L. Laurence</i>	135
Four-Color Proof	136
Goldbach's Conjecture; This One May Be Provable, but We May Never Know <i>George Johnson</i>	137
Mathematics Expert May Soon Resolve A 350-Year Problem <i>James Gleick</i> . .	139
Fermat's Theorem Solved? Not This Time <i>James Gleick</i>	141
Fermat's Last Theorem Still Has 0 Solutions <i>James Gleick</i>	142
At Last, Shout of "Eureka!" in Age-Old Math Mystery <i>Gina Kolata</i>	145
Fermat's Theorem <i>James Gleick</i>	150
Flaw Is Found in Math Proof, but Repairs Are Under Way <i>Gina Kolata</i>	155
A Year Later Fermat's Puzzle Is Still Not Quite Q.E.D. <i>Gina Kolata</i>	157
How a Gap in the Fermat Proof Was Bridged <i>Gina Kolata</i>	158
Two Key Mathematics Questions Answered after Quarter Century <i>John A. Osmundsen</i>	164
Mathematical Theory of Poker Is Applied to Business Problems <i>Will Lissner</i>	169
Soap Bubbles Get a New Role in Old Mathematics Problem <i>Joseph Williams</i>	173
Math Advance Penetrates Secrets of Knots <i>James Gleick</i>	175
Packing Tetrahedrons, and Closing in on a Perfect Fit <i>Kenneth Chang</i>	181
Finding Order in the Apparent Chaos of Currents <i>Bina Venkataraman</i>	184

In Bubbles and Metal, the Art of Shape-Shifting	<i>Kenneth Chang</i>	188
The Scientific Promise of Perfect Symmetry	<i>Kenneth Chang</i>	190
143-Year-Old Problem Still Has Mathematicians Guessing	<i>Bruce Schechter</i>	192
What Is the Most Important Problem in Math Today?	<i>Gina Kolata</i>	196
Solution to Old Puzzle: How Short a Shortcut?	<i>Gina Kolata</i>	198

CHAPTER 4

Chaos, Catastrophe and Randomness

Chaos Is Defined by New Calculus		202
Experts Debate the Prediction of Disasters	<i>Malcolm W. Browne</i>	204
Solving the Mathematical Riddle of Chaos	<i>James Gleick</i>	208
The Man Who Reshaped Geometry	<i>James Gleick</i>	223
Snowflake's Riddle Yields to Probing of Science	<i>James Gleick</i>	235
Tales of Chaos: Tumbling Moons and Unstable Asteroids	<i>James Gleick</i>	239
Fluid Math Made Simple—Sort Of	<i>James Gleick</i>	243
When Chaos Rules the Market	<i>James Gleick</i>	246
New Appreciation of the Complexity in a Flock of Birds	<i>James Gleick</i>	256
Indestructible Wave May Hold Key to Superconductors	<i>James Gleick</i>	261
The Quest for True Randomness Finally Appears Successful	<i>James Gleick</i>	265
Coin-Tossing Computers Found to Show Subtle Bias	<i>Malcolm W. Browne</i>	270
Science Squints at a Future Fogged by Chaotic Uncertainty		
	<i>Malcolm W. Browne</i>	274
Probing Disease Clusters: Easier to Spot Than Prove	<i>Gina Kolata</i>	278
The Odds of That	<i>Lisa Belkin</i>	281
Fractal Vision	<i>James Gleick</i>	298

CHAPTER 5

Cryptography and the Emergence of Truly Unbreakable Codes

Harassment Alleged over Code Research	<i>Malcolm W. Browne</i>	303
Researchers to Permit Pre-Publication Review by U.S.	<i>Richard Severo</i>	306
Tighter Security Rules for Advances in Cryptology	<i>Walter Sullivan</i>	308
A New Approach to Protecting Secrets Is Discovered	<i>James Gleick</i>	312
Brief U.S. Suppression of Proof Stirs Anger		316
A Most Ferocious Math Problem Tamed	<i>Malcolm W. Browne</i>	319
Biggest Division a Giant Leap in Math	<i>Gina Kolata</i>	324

Scientists Devise Math Tool to Break a Protective Code <i>John Markoff</i>	328
Tied Up in Knots, Cryptographers Test Their Limits <i>Gina Kolata</i>	331
A Public Battle over Secret Codes <i>John Markoff</i>	334
U.S. Code Agency Is Jostling for Civilian Turf <i>John Markoff</i>	338
Researchers Demonstrate Computer Code Can Be Broken <i>Sara Robinson</i>	343
Nick Patterson; A Cold War Cryptologist Takes a Crack at Deciphering DNA's Deep Secrets <i>Ingfei Chen</i>	345
Adding Math to List of Security Threats <i>John Markoff</i>	349
Prizes Aside, the P-NP Puzzler Has Consequences <i>John Markoff</i>	351

CHAPTER 6

Computers Enter the World of Mathematics

"Thinking Machine" Does Higher Mathematics; Solves Equations That Take Humans Months.	355
New Giant "Brain" Does Wizard Work	356
"Brain" Speeded Up for War Problems <i>Will Lissner</i>	358
The Electronic Digital Computer: How It Started, How It Works and What It Does <i>Henry L. Lieberman and Dr. Louis Robinson</i>	360
New Shortcut Found for Long Math Proofs <i>Gina Kolata</i>	381
New Technique Stores Images More Efficiently <i>Gina Kolata</i>	385
Giant Computer Virtually Conquers Space and Time <i>George Johnson</i>	390
Rear Adm. Grace M. Hopper Dies; Innovator in Computers Was 85 <i>John Markoff</i>	395
Frances E. Holberton, 84, Early Computer Programmer <i>Steve Lohr</i>	398
Squeezing Data like an Accordion <i>Peter Wayner</i>	400
A Digital Brain Makes Connections <i>Anne Eisenberg</i>	403
A Soviet Discovery Rocks World of Mathematics <i>Malcolm W. Browne</i>	406
The Health Care Debate: Finding What Works <i>Gina Kolata</i>	410
Step 1: Post Elusive Proof. Step 2: Watch Fireworks. <i>John Markoff</i>	415

CHAPTER 7

Mathematicians and Their World

Paul Erdos, 83, a Wayfarer in Math's Vanguard, Is Dead	<i>Gina Kolata</i>	420
Journeys to the Distant Fields of Prime	<i>Kenneth Chang</i>	423
Highest Honor in Mathematics Is Refused	<i>Kenneth Chang</i>	428
Scientist at Work: John H. Conway; At Home in the Elusive World of Mathematics	<i>Gina Kolata</i>	430
Claude Shannon, B. 1916—Bit Player	<i>James Gleick</i>	436
An Isolated Genius Is Given His Due	<i>James Gleick</i>	438
Scientist at Work: Andrew Wiles; Math Whiz Who Battled 350-Year-Old Problem	<i>Gina Kolata</i>	444
Scientist at Work: Leonard Adleman; Hitting the High Spots of Computer Theory	<i>Gina Kolata</i>	449
Dr. Kurt Gödel, 71, Mathematician	<i>Peter B. Flint</i>	456
Genius or Gibberish? The Strange World of the Math Crank	<i>George Johnson</i>	458
Contributors' Biographies	463
Photography and Illustration Credits	467
Acknowledgments	468
Index	469

FOREWORD

*A formidable student at Trinity
Solved the square root of infinity;
It gave him such fidgets
To count up the digits
He chucked math and took up divinity.*

—Anonymous

This old limerick, penned by an anonymous wag, encapsulates two fundamental characteristics of mathematics and at least one misconception. The limerick correctly portrays mathematics as addressing big, head-spinning notions like that of infinity, and it gets across the fact that mathematical concepts can be difficult for laymen to comprehend. But the verse wrongly suggests that counting is the essence of mathematics. Counting is for bank tellers, cashiers, and CPAs. As the *Times* articles in this book make clear, mathematicians do much more than arithmetic. They are on the hunt for eternal universal truths, a quest that a budding theologian at Trinity would appreciate.

Around 300 B.C., Euclid of Alexandria offered a simple proof that there are infinitely many prime numbers (integers like 3, 5, 7, 11, and 13 that are divisible only by themselves and the number 1). His proof is as true today as it was twenty-three hundred years ago, and it will be true twenty-three hundred years from now. This kind of categorical certainty makes mathematics unique among the sciences. No matter how far out we go in the number line (beyond a hundred million, or a hundred million million, or a hundred million million million) there will always be primes. The “truths” of physics are not so universal. The discoveries of Newton and Einstein seem to hold only at certain familiar scales and not at “far out” distances.

More than the other sciences, mathematics seems to pose an abundance of simple questions that are beyond current human ingenuity. To take but one example in number theory, there is the unsolved puzzle of whether the supply of so-called twin primes (pairs of primes that differ by two, such as 3 and 5, 17 and 19, and 3,581 and 3,583) is inexhaustible. Although Euclid proved that the number of primes is infinite, generations of mathematicians have not been able to

prove their suspicion that the number of twin primes is also infinite. Euclid's proof is so simple that it can be written on one side of an index card. This raises the deep meta-mathematical question of why certain seemingly simple mathematical questions are maddeningly intractable compared to other related questions that readily give up their answers.

Contemporary mathematics is still about the search for eternal truths, but mathematicians now have a wider repertoire of techniques for getting at these truths. Chief among these is the computer, which itself is the product of mathematics, the binary language of 0s and 1s. I was in college in the mid 1970s when my professors at Harvard received word that two mathematicians in the Midwest had proved the century-old four-color conjecture, which asserts that any imaginary map of countries can always be colored with at most four colors in such a way that no two bordering countries share the same color. A lot of champagne was poured in the Harvard math department, but jubilation later gave way to consternation when word got out that the proof involved a computer doing much of the heavy lifting. It wasn't that my professors distrusted the proof; they presumed that the correctness of its numerous steps could be confirmed by running the proof on another machine. They were disquieted by the fact that the proof was so long that no human being would be able to assimilate it and understand *why* four colors were sufficient. For them a proof had to provide insight, and in this regard Euclid's half-page proof was the gold standard: they could easily follow it and understand *why* the number of primes was infinite.

You'll learn from the *Times* articles within about the four-color conjecture and other intriguing mathematical conundrums that computers have helped to solve (for example, the party planner's problem of determining the minimum number of guests that must be invited to guarantee that eight or more guests all know one another and that three or more will be strangers) and the meta issues such computer-aided proofs raise. You'll also find stories about famous problems such as Fermat's Last Theorem and the Poincaré conjecture that were recently proved the old-fashioned way, without depending on machines.

The men you'll meet in these pages (and I say men, because few of these mathematicians are women) include other worldly eccentrics like Grigori Perelman, who solved the century-old Poincaré conjecture only to retreat into the Russian woods, turning down both a \$1-million reward and the Fields Medal, the equivalent in mathematics of the Nobel Prize, and Paul Erdos, arguably the world's most prolific mathematician, a homeless Hungarian who, jacked up on

FOREWORD

amphetamines and espresso, worked on problems twenty hours a day and published more than 1,500 papers. "Mathematicians are machines for turning coffee into theorems," Erdos would say. When colleagues asked him to slow down, he'd reply, "They'll be plenty of time to rest in the grave." Erdos died at the age of eighty-three, but his mathematics, like all mathematics, is immortal. The discoveries he made, like Euclid's and Grigori's, will hold up for eternity.

Paul Hoffman
CEO of Liberty Science Center and author of
The Man Who Loved Only Numbers

INTRODUCTION

A mathematician once dismissed the very idea that people outside his circle could ever understand the true essence of the field. Mathematics is an art form, like music or painting. Translating math into the English language, he said, is harder than translating Chinese poetry. The beauty is lost, the elegance, and a proof that is a thing of ineffable iridescence becomes reduced to a baffling or mundane-sounding bottom line.

Others echoed that sentiment. Fritz John, a mathematician at New York University, said he wanted neither fame nor fortune but merely “the grudging admiration of a few close friends.”

But even if the rest of us cannot appreciate mathematics as an art form, are we really shut out? Articles in *The New York Times* may not give the details of proofs, but they reveal a rich world that can be exciting, surprising, and can even tug at the heartstrings. They even address the age-old question, What is mathematics? Is it discovered or is it invented? Art or science? If it is art, then why, as George Johnson wrote in one of the articles that opens this book, does the universe appear to follow mathematical laws?

Yet if we put philosophy aside, the variety of mathematical questions, the scope of its inquiries as reported in the *Times*, can be stunning. There are articles that give mathematical solutions to everyday questions—why do heavy objects rise to the top of a container? The strawberries in your jam are all at the top of the jar so when you get toward the bottom, all you have is thick syrup. Brazil nuts are at the top of the mixed nuts can. A mathematical discovery tells why.

Or what about the woman who won the New Jersey lottery twice in four months? The odds of that happening were widely reported as 1 in 17 trillion. But actually, statisticians calculated, they were more like 1 in 30. A *Times* article tells how to reason through such questions.

And does arthritis pain really respond to changes in the weather? Statisticians answer that one, too, with an analysis that makes sense but confounds perceptions. Another article tells of a surprising result in controlling traffic jams—mathematicians can prove that sometimes closing streets actually improves traffic flow.

But while those articles can make us look at the world differently, they are not about results that rocked mathematics. If you asked mathematicians which proofs

were most important to them, many would cite the surprising, drama-laden tales of the search for solutions to some of their most famous problems. And the story of Fermat's Last Theorem would be at the top of many lists. Nearly 400 years ago, a French mathematician scrawled the problem in the margins of a book, saying he had a simple proof but no space to write it. Ever since, mathematicians tried to solve it, to no avail. Some famous mathematicians said they would not even take it up—it was a fool's errand, they would just waste precious years of their lives only to end up empty-handed.

Then, in 1993, a young mathematician, Andrew Wiles, announced that he had solved Fermat. What followed was elation, followed by intense questioning. It was a complicated proof, relying on recently discovered mathematics that few truly understood. And as mathematicians scrutinized Wiles's work, they found a hole in the proof, which Wiles then desperately tried to fix. He retreated to a barren office in his attic, where he had secretly done his work, attempting to make the proof whole again. It was a year of drama that ended well, but the roller-coaster tale, told in the pages of the *Times* as it happened, was an unforgettable story of pride and ambition, talent and determination.

Not all mathematics is logical, and researchers have wondered how to describe the unpredictable, like the famous analogy of the Butterfly Effect, described by mathematician Edward Lorenz in a lecture in 1972 titled "Does the Flap of a Butterfly's Wings in Brazil Set Off a Tornado in Texas?" As mathematicians tried to understand such phenomena, they developed the new fields, or newly named fields, chaos theory and catastrophe theory. And with those fields came debate. Were the results overstated? How predictable were some of these events? And what can the research say about important questions, like global warming, which involve some of the same uncertainties?

Other articles involve discoveries that changed the way we live and work. In the 1980s, a few mathematicians had a brilliant idea for making unbreakable secret codes. There are some problems that are simple to check once you have the answer, but pretty much impossible to solve unless you have centuries or millennia to run your computer. One such problem is factoring—figuring out which prime numbers can be multiplied together to make a particular number. You can easily multiply, say 3 times 5 times 11 times 13 to get 2,145, but it is a bit more work to start with 2,145 and find those factors. The codes, though, use enormous numbers, not simple ones like 2,145. And with huge numbers, there is no easy way to get the factors. So, suppose you made a code that required you

to factor a large number if you wanted to break it. You could send a message by doing the equivalent of multiplying a large group of prime numbers together. And no one could illicitly read that message without factoring the resulting huge number.

The idea was so powerful that the federal government got alarmed at mathematicians' proclivities to publish all of their work, leading to a difficult national debate about how much can or should be revealed. Some said it was important for the codes to be public in order to use them to keep sensitive information, like credit card transactions, private. Others said it was important to keep coding methods secret so enemies could not use them and make codes that the government could not break. In the end, the methods became an integral part of today's online world, allowing, for example, the secure Web sites we use when we shop online. The *Times* articles tell the story of the discoveries and the wrenching debate.

Although many fields of science today involve huge teams of researchers, mathematicians often work alone. One brilliant person can change a field. And many of these mathematicians have stories and insights that can be unforgettable. The *Times* articles include the haunting story of Srinivasa Ramanujan, born in the 19th century in a small town in India, who died at age 32. He left "a strange, raw legacy, about 4,000 formulas written on the pages of three notebooks and some scrap paper." His extraordinary story—how he was discovered, how inventive he was—is a tale like no other. "He seemed to have functioned in a way unlike anybody else we know of," one mathematician said. "He had such a feel for things that they just flowed out of his brain. Perhaps he didn't see them in way that's translatable. It's like watching somebody at a feast that you haven't been invited to."

Contemporary mathematicians can tell us what it might feel like to be part of their feast. Leonard Adleman, one of the inventors of the new type of secret code, discovered in graduate school that mathematics "is less related to accounting than it is to philosophy." While many "think of mathematics as some kind of practical art," he said, "the point when you become a mathematician is when you somehow see through this and see the beauty and power of mathematics."

Some, not surprisingly, are just odd people, geniuses but eccentric almost beyond belief. That, at least, describes Paul Erdos, a Hungarian mathematician who had no home and no job. Other mathematicians invited him into their homes, feeding and housing him—and collaborating with him—until he moved

INTRODUCTION

on to another mathematician's home. He also took on the question that opens this book. Are mathematical truths discovered or invented? Erdos said they were discovered. As I wrote in an obituary about this unforgettable man, Erdos "spoke of a Great Book in the sky, maintained by God, that contained the most elegant proofs of every mathematical problem. He used to joke about what he might find if he could just have a glimpse of that book."

Gina Kolata



CHAPTER 1

What Is Mathematics?

MATHEMATICIANS SOMETIMES ASK THEMSELVES IF THEY are finding truths about the real world or indulging in creative inventions. Is mathematics an art or a science? Often someone will cite an article by the physicist Eugene Wigner, published in 1960 and titled "The Unreasonable Effectiveness of Mathematics in the Natural Sciences." Mathematics, Wigner wrote, is almost uncannily effective in describing physical phenomena. And so, he wrote, "The miracle of the appropriateness of the language of mathematics for the formulation of the laws of physics is a wonderful gift which we neither understand nor deserve. We should be grateful for it and hope that it will remain valid in future research and that it will extend, for better or for worse, to our pleasure, even though perhaps also to our bafflement, to wide branches of learning."

In this section, George Johnson takes this issue of the nature of mathematics. He tells of the argument of an eminent mathematician, Reuben Hersh, that mathematics is invented. He quotes Einstein, who said humans invented mathematical tools that allowed us to describe nature but were not, in fact, an essential truth.

Jim Gleick addresses a closely related issue. What is mathematics good for? Is it enough to say that mathematics, discovered or invented, should just be pursued for its own sake, with applications coming later?

Is it enough to evoke the Wigner argument—if mathematical truths are found they will turn out to be “unreasonably effective” in describing the natural world?

Or what if a computer, an unthinking computer, could spew out mathematical ideas or even produce proofs that would be considered creative if a human produced them? What does that do to the idea of mathematics as an art form?

There is no consensus in these articles, but they abound with provocative insights and questions.

Useful Invention or Absolute Truth: What Is Math?

By GEORGE JOHNSON

At the top of the list of science's unanswered questions, like what is consciousness and how did life begin, is the deepest mystery of all: Why does the universe appear to follow mathematical laws?

According to the Big Bang theory, matter, energy, space and time were created during the primeval explosion. Instantly, it seems, everything began unfolding according to a mathematical plan. But where did the mathematics come from? What are the origins of numbers and the relationships they obey?

The ancient followers of the Greek mathematician Pythagoras declared that numbers were the basic elements of the universe. Ever since, scientists have embraced a kind of mathematical creationism: God is a great mathematician, who declared, "Let there be numbers!" before getting around to "let there be light!"

Scientists usually use the notion of God metaphorically. But ultimately, most of them at least tacitly embrace the philosophy of Plato, who proposed, rather unscientifically, that numbers and mathematical laws are ethereal ideals, existing outside of space and time in a realm beyond the reach of humankind.

Because the whole point of science is to describe the universe without invoking the supernatural, the failure to explain rationally the "unreasonable effectiveness of mathematics," as the physicist Eugene Wigner once put it, is something of a scandal, an enormous gap in human understanding.

"We refuse to face this embarrassment," Reuben Hersh, a mathematician emeritus of the University of New Mexico in Albuquerque, wrote in his recent book, *What Is Mathematics Really?* (Oxford University Press, 1997). "Ideal entities independent of human consciousness violate the empiricism of modern science." While science is anchored in observations of the physical world, Dr. Hersh insists that mathematics is more of a human creation, like literature, religion or banking.

Dr. Hersh's book is one of several recent works contending that mathematics is not an ethereal essence but comes from people who invented, not discovered, it. The sentiments presented in the books are not entirely new and the mathematical puzzle has hardly been solved. But the idea of a human-centered mathematics may be gaining force and respect.

In *The Number Sense: How the Mind Creates Mathematics* (Oxford University Press, 1997), Stanislas Dehaene, a cognitive scientist at the National Institute of Health and Medical Research in Paris, marshals experimental evidence to show that the brains of humans—and even of chimpanzees and rats—may come equipped at birth with an innate, wired-in aptitude for mathematics. Gregory J. Chaitin, a mathematician at I.B.M.'s Thomas J. Watson Research Center in Yorktown Heights, N.Y., takes an anti-Platonist stance in *The Limits of Mathematics* (Springer, 1997). Two Berkeley scientists, George Lakoff and Rafael E. Núñez, are working on a book tentatively called *The Mathematical Body*, contending that even the most abstract mathematical concepts arise from basic human experience—from the way the body interacts with the world. They gave a preview of their ideas in a chapter of another book published last year: *Mathematical Reasoning: Analogies, Metaphors and Images*, edited by Lyn D. English (Erlbaum).

The authors are all working mathematicians and scientists, not postmodern critics viewing the territory from afar. They emphatically reject those who try to dismiss mathematics and science as arbitrary constructions, or white male Eurocentric folklore. But they are just as adamant in rejecting what most mathematicians and many scientists have come to take for granted: the Platonic creed.

"The normal notion of pure math is that mathematicians have some kind of direct pipeline to God's thoughts, to absolute truth," Dr. Chaitin wrote in *The Limits of Mathematics*. While scientific knowledge is tentative and subject to constant revision, mathematics is usually seen as eternal. But Dr. Chaitin called on his colleagues to abandon mathematical Platonism and adopt a "quasi-empirical" approach that treats mathematics as just another messy experimental science.

"Quasi-empirical," he said, "means that math ain't that different from physics." This view is laid out in detail in a revised edition of *New Directions in the Philosophy of Mathematics*, edited by Thomas Tymoczko (Princeton University Press, 1998).

Leopold Kronecker, a 19th-century mathematician, once said: "The integers were created by God; all else is the work of man." Albert Einstein, taking a different view of whole numbers, wrote that "the series of integers is obviously an invention of the human mind, a self-created tool which simplifies the ordering of certain sensory experiences."

In *The Number Sense*, Dr. Dehaene went even further. The integers—the smallest ones, anyway—are hard-wired into human nervous systems by

evolution, along with a crude ability to add and subtract. Mathematics, he believes, is "engraved in the very architecture of our brains."

"Because we live in a world full of discrete and movable objects, it is very useful for us to be able to extract number," he argued in a recent forum published on the Internet (www.edge.org) by the Edge Foundation. "This can help us to track predators or to select the best foraging grounds, to mention only very obvious examples."

By studying brain-damaged patients who have lost basic number skills, Dr. Dehaene and others have tentatively traced this arithmetical module to an area of the brain called the inferior parietal cortex, a poorly understood location where visual, auditory and tactile signals converge. Scientists are intrigued by clues that this region is also involved in language processing and in distinguishing right from left. Mathematics is, after all, a kind of language intimately involved with using numbers to order space. The inferior parietal cortex also seems to be important for manual dexterity, and arithmetic begins with counting on the hands. Imaging experiments, in which people's brains are monitored as they calculate, point to the same region as a primitive number processor.

If this neurological calculator has indeed been bequeathed by evolution, then traces of it should be found in other species. In making his argument, Dr. Dehaene draws on experiments over the last few decades suggesting that even rats have a rudimentary number sense. The animals were taught to press lever A four times and then lever B to get food, or to press lever A when they heard a two-tone sequence and lever B when they heard an eight-tone sequence. (To insure that the rats were responding to the number of signals and not just to their duration, the two-tone sequence sometimes lasted longer than the eight-tone one.)

Even more striking were later experiments in which rats were first trained to associate lever A with two tones and lever B with four tones. Then they were taught to associate A with two flashes of light and B with four flashes. If the rats heard two tones and saw two flashes they learned to push B, not A. They seemed to have comprehended the notion that two plus two equals four.

The rats were not precise. Trained to press one lever four times, they often pressed it five or six times, expecting to be rewarded just the same, or they confused a seven-tone sequence with an eight-tone one. But the experiments support the notion of a primitive neurological number processor, even in rodents.

In other experiments, chimpanzees seemed to learn simple arithmetic. Given a choice between one tray with a pile of three chocolate chips and another pile

of four and a second tray with piles of two and three chips, they chose the first tray with the most candy. But when the totals on the trays differed by only one chip, the chimps were less likely to make the discrimination. The number sense is approximate, not exact. More recent experiments on infants, using Mickey Mouse toys instead of chocolate chips, found signs of the same kind of rough numerical ability in babies less than 5 months old.

Dr. Dehaene says this instinct is innate, as singing is for songbirds or spinning webs is for spiders. Numbers are not Platonic ideals but neurological creations, artifacts of the way the brain parses the world. In that sense they are like colors. Red apples are not inherently red. They reflect light at wavelengths that the brain, as it was wired by evolution, interprets as red.

While people are born with an understanding of the rudiments of arithmetic, he contends, going beyond that requires learning and creativity. Multiplication, division and the whole superstructure of higher mathematics—from algebra and trigonometry, to calculus, fractal geometry and beyond—are a beautiful improvisation, the work of human culture.

The ability to weave simple ideas, like two plus two equals four, into the tapestries of higher mathematics, he suggests, is not unlike the human skill for language. People take a relatively small collection of words and, using a few simple rules of grammar and syntax, create literature.

At the University of California at Berkeley, Dr. Lakoff, a linguist and cognitive scientist, and Dr. Núñez, a developmental psychologist, contend that the source of mathematics lies not just in the brain but in the human body and the physical world. People favor number systems based on 10 because they have 10 fingers and 10 toes. But that is just the beginning of the story.

Driven by a built-in number sense, the theory goes, primitive people explored the wonders of counting by playing with their fingers or putting rocks in a pile. But they found that counting could also be thought of as taking steps along a line to measure distance. That metaphor eventually allowed for the invention of more abstract concepts. Walk one way and you get the positive integers; walk the other way and you get the negative integers. The starting point is zero.

Multiplication by a positive number can be thought of as stretching; multiplying by a negative number makes something shrink.

Dr. Lakoff and Dr. Núñez call these “grounding metaphors.” In inventing mathematics, they contend, people also used “linking metaphors” to connect two sets of ideas. The sequence of numbers can be mapped onto the notion of

a line. Now numbers are not fingers or rocks but points. Put two lines together at right angles and you get what mathematicians call a Cartesian plane, a two-dimensional graph that opens up a whole new arena to play in.

And so, floor by floor, the tower of mathematics is built. "Students never learn that mathematics is a creative endeavor," Dr. Lakoff said in a recent interview. "Mathematics is more glorious because it is humanly constructed." There is no such thing as pure mathematics or pure thought, he said—they are physical activities.

That does not mean that mathematics is a relativistic free-for-all. The most basic mathematical inventions are rooted in the brain and body. Even mathematicians' loftier elaborations are tested against the universe. Of the infinite range of mathematical creations, scientists keep those that help them explain and predict reality. Mathematicians savor the others as ends in themselves, like paintings or symphonies.

But many scientists and mathematicians still doubt that evolution—biological or cultural—can adequately explain why mathematics works so well in describing the fundamental laws of the universe.

"Our ability to discover, and describe mathematically, Newton's equations has no immediate survival value," said Dr. Paul Davies, professor of mathematical physics at the University of Adelaide in Australia. "This point has even greater force when it comes to, say, quantum mechanics. The reason people find it hard to understand quantum physics is precisely because there is no survival value in being able to do so."

The reason mathematics is so effective, he says, remains a deep mystery. "No feature of this uncanny 'tuning' of the human mind to the workings of nature is more striking than mathematics," he wrote in *The Mind of God: The Scientific Basis for a Rational World* (Simon & Schuster, 1992).

Some hold out vague hopes that the mystery might be solved if humans ever encounter an alien civilization. If mathematics is indeed universal and eternal, the theory goes, then the aliens would understand concepts like pi, the ratio of a circle's circumference to its diameter. The Platonists assume that there is "pi in the sky," as the British astronomer John D. Barrow said in a book by that name (Oxford University Press, 1992).

The anti-Platonists say there is no reason to believe the aliens would understand mathematical inventions from Earth. "The Platonist claim that every intelligence must produce prime numbers, pi and the continuum hypothesis is an example of simple anthropomorphism," Dr. Hersch said.

But if earthlings were utterly baffled by extraterrestrial mathematics, would the anti-Platonists have proved their point? Not necessarily.

"Alien intelligences may be so far advanced that their math would simply be too hard for us to grasp," Dr. Davies said. "The calculus would have baffled Pythagoras, but with suitable tuition he would have accepted it."

But what if the humans and the aliens could communicate mathematically? Would that decide the issue in favor of the Platonists? Not really.

"If the alien species had evolved in an environment similar to ours—say, a world composed of distinct, movable objects—then most likely its brain would have incorporated, through natural selection, the same regularities about the external world as we have," Dr. Dehaene said. "Thus, it would have a very similar arithmetic and geometry.

"But now, suppose that the alien species has evolved in a radically different environment, like a fluid world," he continued. "Then knowledge of movable objects would not be essential to its survival, while knowledge of fluid mechanics, vortices, etc. would be. I believe that this hypothetical species would have internalized in its brain regularities strikingly different from ours. Hence it would have radically different mathematics."

And so the argument continues to churn.

Several years ago, the French mathematician Alain Connes, arguing for the Platonists, and the French neurobiologist Jean-Pierre Changeux, taking the opposite side, tried to settle the matter with a debate. The result, translated and edited by M. B. DeBevoise, was the book *Conversations on Mind, Matter and Mathematics* (Princeton University Press, 1995).

Ranging over a vast field of topics including relativity, quantum mechanics, neurobiology, topology, game theory, information theory and non-Euclidean geometry, the two reached the end of their discussion with no resolution.

The best they could do was to agree to disagree.

February 11, 1998

But Aren't Truth and Beauty Supposed to be Enough?

By JAMES GLEICK

Could the mathematicians, winners of the most prestigious awards of their discipline, please tell the audience what their work is good for?

Flush with pleasure, these four young men, carrying home three Fields Medals and a Nevanlinna Prize, were telling a lay audience what their work was about. Two had discovered astonishing facts about shapes in four-dimensional space. One had developed important insights into what makes hard problems hard. One had proved the Mordell conjecture, the idea that a large class of equations can have only a finite number of rational solutions.

To the nearly 4,000 mathematicians who gathered here for the International Congress of Mathematicians, which ended Monday, these were an astonishing set of breakthroughs demonstrating new vitality in the purest of sciences. But a reporter-cameraman for a local television station wanted at least one of the prize winners to address a basic question: How would their achievements improve life for the viewers at home?

Embarrassed silence. The mathematicians suddenly seemed to have remembered pressing engagements elsewhere. They looked at one another. Gerd Faltings, a boyish, blond West German who became one of mathematics' great men when he proved the Mordell conjecture, gave an awkward smile and flatly refused to speak.

It was Michael Freedman, a topologist in California, who rose in the end to say what all the mathematicians felt: That theirs is a way of thinking that thrives by disdaining the need for practical applications. Let the applications come later by accident—they always do. A weird, curved parody of Euclidean geometry turns out to be just the framework a physicist needs to invent the General Theory of Relativity. Notoriously unpractical techniques of number theory turn out to be just what the National Security Agency needs to make efficient, secure codes.

Usually unspoken, but always present, is the faith that doing mathematics purely, following an internal compass, seeking elegance and beauty in a strange abstract world, is the best way in the long run to serve practical science. As physics or biology progress, they will inevitably find that the way ahead has been cleared

by some odd piece of pure mathematics that was thought dead and buried for many decades.

"We're a part of a gigantic enterprise that has gone on for hundreds of years, and interacts in interesting ways with science, and operates on a very low budget," Dr. Freedman said, "and we've learned that it's hard to prophesy what piece of mathematics will have what particular applications. Mathematics has to advance as an organic whole, in ways that seem right to the people inside it."

An older mathematician, Sir Michael Atiyah of Oxford University, who won a Fields Medal himself in 1966, offered one correction. "It's been thousands of years," he said. "So we're in business on a long-term basis."

Yet the meaning of mathematical purity is changing—has changed, many mathematicians said, even since the last Congress in Warsaw in 1983. Questions about the nature of that change, and what it might mean for the future, hovered in the air through 16 "plenary addresses," scores of 45-minute lectures and hundreds of 10-minute "short communications" in the nine-day conference.

Mostly unrepresented was the somewhat less exalted discipline known as applied mathematics, the traditional route for mathematical ideas to filter down to engineering and other sciences. A few mathematicians could not help noticing, though, that recently physical scientists have been plucking ideas directly from the heart of pure mathematics, bypassing applied mathematics altogether. Many unexpected connections have arisen—between knot theory and genetic processes in DNA strands, for example—but the most important has been the use of geometric ideas in the theory of cosmic strings, the hottest new game in the physics of fundamental forces and particles.

The suspicion of a few mathematicians here was that biologists and chemists can no longer be relied on to be naive about the arcana of number theory or topology. That will take some getting used to.

And in the case of strings, the physics has begun feeding back into mathematics, meaning that the up-to-date pure mathematician may now have to learn some unpure science. This state of affairs was highlighted by two unusual talks by physicists Edward Witten of Princeton University and Aleksandr Polyakov of the Soviet Union's Landau Institute for Theoretical Physics.

Dr. Polyakov, an intense man with long sandy hair, paced nervously before his lecture, a red knapsack on his back. He was worried that his mathematician audience would be put off by having to hear a foreign language—physics, not Russian.

"I apologize if you are irritated by the reckless manner of a physicist," he told his audience. Reckless, because the two disciplines have different standards of proof: A physicist is content to say that the earth orbits the sun; a mathematician will say only that there is convincing evidence.

Dr. Freedman, in the work that won his Fields Medal, proved that certain exotic four-dimensional spaces exist. Another medalist, Simon Donaldson of Oxford, meanwhile, used tools from physics to prove that these same spaces could not exist.

"So the conclusion a mathematician would draw," Dr. Freedman said, "is that physics doesn't exist."

To some mathematicians, purity has always meant a certain degree of inscrutability. That, at least, has not changed.

Sometimes inscrutability comes with the territory—for example, when the territory has four dimensions or more. A mathematician needs to be comfortable with shapes in many dimensions, but not everyone can actually visualize more than the usual three. That is one reason geometry relies, for the sake of purity, on rigorous proofs using numbers and symbols. Visual imagination cannot be trusted.

One dimension is a line. The second dimension comes when you add a second line at right angles to the first, so that now you have east-west and north-south. The third dimension requires a new line at right angles to the others, so you must leave the flat plain and draw one up-down. To imagine a fourth dimension, it is necessary to imagine a fourth line at right angles to all the others, and this most mortals cannot do.

Yet some kind of inner vision led John Milnor of the Institute for Advanced Study in Princeton, in describing the four-dimensional discoveries of Dr. Freedman to an audience of several thousand, to start gesturing with his hands.

"The problem is," he was saying, "when you try to embed a two-dimensional disk inside a four-dimensional manifold, it will usually intersect itself." His hands formed loops and handles in the air, as though he were describing some new kind of suitcase.

Sometimes inscrutability is just a matter of style.

It has been said that the ideal mathematics talk has three parts. The first part should be understood by most of your audience. The second part should be understood by four or five specialists in your field. The third part should be understood by no one—because how else will people know you are serious?

Some speakers seemed to follow these guidelines, mathematicians felt. Others, perhaps to save time, skipped directly to part three.

There was one question that the Fields Medalists could not wait to answer, and that was whether they used computers, the unloved child of mathematics and an object whose influence was more in evidence at the Congress than ever before.

"No," Dr. Freedman said. Dr. Donaldson: "No." Dr. Faltings said, "Perhaps it could reduce some sorts of tedious work for us, but it doesn't do the thinking." Personally he doesn't use one.

Eyes turned to Leslie G. Valiant of Harvard University, winner of the recently established Nevanlinna Prize for Information Science, whose work centered on computer algorithms. "Maybe I should clarify my own position," Dr. Valiant said. "I don't use computers either."

If the mathematicians were inclined toward parable and metaphor—and they most definitely are not—they might describe a vast wilderness, and in it a small society of men and women whose business it is to lay railroad track. This has become an art, and they have become artists—artists of track, lovers of track, connoisseurs of track.

Almost perversely, they ignore the landscape around them. A network of track may head to the northeast for many years and then be abandoned. An old, nearly forgotten line to the south may sprout new branches, heading toward a horizon that the tracklayers seem unable or unwilling to see.

As long as each new piece of track is carefully joined to the old, so that the progression is never broken, an odd thing happens. People come along hoping to explore this forest or that desert, and they find that a certain stretch of track takes them exactly where they need to go. The tracklayers, for their part, may have long since abandoned that place. But the track remains, and track, of course, is the stuff on which the engines of knowledge roll forward.

August 12, 1986

Mathematicians Meet Computerized Ideas

By GINA KOLATA

Suppose a computer program could give artists their ideas for what to paint. Or what if a computer program churned out possible story ideas for novelists? Would anyone want to use them?

Mathematicians, many of whom consider themselves more artists than scientists, have had to consider exactly this problem. A researcher has devised a program that spews out conjectures in a field of mathematics known as graph theory.

A conjecture is to a mathematician what a hypothesis is to a scientist: an educated guess to be tested for possible canonization into the realm of truth.

"Finding a good conjecture is definitely half of the job," said Siemion Fajtlowicz, the University of Houston mathematics professor who wrote the program, called Graffiti. The program can easily generate tens of thousands of conjectures, he said. Although some mathematicians have been happy to work on proving the conjectures true or false, others seem to resent the computer, Dr. Fajtlowicz said. "I've run into quite a few Luddites," he said.

Although Dr. Fajtlowicz has been promoting his program at math meetings, throwing out conjectures and hoping that his colleagues or students would become interested in trying to prove them, most mathematicians, even graph theorists, have still not heard of it. It remains a somewhat bizarre source of mathematical inspiration and an irritant to some researchers.

One mathematician told Dr. Fajtlowicz he was furious that the computer had chanced upon a mathematical truth that he himself had discovered. Another mathematician wrote to Dr. Fajtlowicz, only half in jest, that Graffiti was putting him out of a job.

Seeking Truths

Dr. Fajtlowicz said his computer program starts with a collection of graphs, which are groups of points connected by lines. A highway road map is a graph, for example. The program looks for relationships that seem to hold true for the graphs in its collection and then proposes them as more general truths.

In a way, it is like the story of the monkeys banging away at typewriters. Sooner or later, one will type *Hamlet*. And sooner or later, Graffiti will find important mathematical truths by randomly trying many different relationships. But the challenge, Dr. Fajtlowicz said, is to find that mathematical work of art when it appears. "The difficult thing is to discard everything else but *Hamlet*," he said.

So Dr. Fajtlowicz had to decide what made a good conjecture. He said he could not simply ask the program to spit out every conjecture it could find because he would soon be buried in a pile of mostly uninteresting ones. One round of Graffiti results in 3,000 to 8,000 conjectures.

The trick was to find a way to automate a mathematician's instinctive feeling that some possibilities are more worthy of study than others. But mathematicians describe the act of research as highly creative and say they are guided by an intuitive sense of what is significant and what is not. They often describe a theorem they like as beautiful and a particularly striking proof as elegant.

"I asked everybody in sight, 'How do you know if a conjecture is interesting?'" Dr. Fajtlowicz said. "Nobody seemed to know."

He eventually chose four criteria. A conjecture would have to be surprising, judged by how different it was from conjectures the computer had made before. It could not be a logical consequence of another conjecture. It should not be overly specific. And if a conjecture compared two quantities, the quantities should be close in size. Using these standards, he was able to eliminate all but 20 to 50 of the proposals produced by a run of the program.

Dr. Fajtlowicz said that at least 20 mathematicians have worked on proving conjectures generated by the program and that he knows of five papers proving Graffiti conjectures that have either been published or accepted for publication by mathematics journals.

Fan Chung, who directs research in mathematics and communications at Bell Communications Research in Morristown, N.J., has worked on a Graffiti conjecture. She described it as a statement about two properties of a graph. One is the average distance between pairs of points. The other is a quantity called the independence number, which has to do with how many areas of the graph are not adjacent to one another. The conjecture said that if the average distance is large, so is the independence number.

"What attracted me to the conjecture was its simplicity," Dr. Chung said. "It was a very clean relationship. But it was harder to prove than it first looked."

Dr. Chung said that given a choice, she would rather work on her own conjectures or on those that have gained a certain fame or notoriety in mathematics because they have been so difficult to verify. But, she added, "It doesn't bother me" to work on a problem suggested by a machine.

Dr. Fajtlowicz said that the more he has worked with Graffiti, the more he appreciates its abilities. "I think Graffiti is good at generating problems," he said. "In fact, I think now it is better than me."

June 18, 1989

Mathematicians Finally Log On

By JAMES GLEICK

Computers crunch numbers, make pictures, store data and perform arithmetic, and that is why pure mathematicians have long abhorred them.

Mathematicians do not calculate; they think. University mathematics departments have been pretty much the last holdouts in science against the encroachment of computers, and mathematicians the last holdouts against tools more advanced than pencil and paper.

So, many mathematicians are being surprised, and not always cheerfully, to see computation forcing profound changes in the place where it started, the heart of pure mathematics. The computer is being used for experimentation, itself an alien notion to most mathematicians. It is creating new fields within mathematics. And it may be changing the nature of mathematical proof.

"In the sort of stuff pure mathematicians do, the computer as a research tool is still very much of a novelty, but that's changing extremely rapidly," said David A. Hoffman of the University of Massachusetts at Amherst. Dr. Hoffman and his colleagues have used the graphics-producing ability of computers to overthrow some century-old beliefs about abstract geometries with applications to chemistry and physics.

Such discoveries have led program managers at the National Science Foundation and in the military's research offices to change their attitude toward financing computation in pure mathematics. "Computational mathematics" is becoming a subject in its own right. At the International Congress of Mathematicians this month in Berkeley, Calif., signs of the computer were everywhere. The opening plenary speaker, Stephen Smale of the University of California at Berkeley—a pure mathematician with a record of bringing fellow mathematicians into new areas—focused on the developing theory of complexity, which addresses questions of what sorts of problems can and cannot be solved on computers.

The problem-solving abilities of computers, Dr. Smale said, have created a challenge that is philosophical, logical and mathematical. "This subject is now likely to change mathematics itself," he said. "Algorithms become an object of study, not just a means of solving problems." A Laboratory Instrument Complexity theory is bringing computer science and information science into the mainstream

of mathematics, but for some mathematicians, still in the minority, the most important effect of computers has been the creation of a new style of working. In effect, the computer is the first laboratory instrument that mathematicians have ever had. Dr. Hoffman of the University of Massachusetts is an example. He was studying an old theoretical problem in differential geometry, that of minimal surfaces. A minimal surface is the smallest possible area that can stretch over a given shape—for example, the surface defined by a soap film stretched on a wire frame.

Mathematicians have long pursued an abstract class of these structures known as infinite, complete minimal surfaces—a class that they thought had only three members, a flat plane, a spiral and an hourglass shape. The study has direct implications for architecture, where it affects the design of strong, light structures, and for the chemistry of polymers, substances with long chains of molecules. At a deeper level, these geometrical surfaces correspond to equations used in problems from the flow of fluids to the theory of relativity.

Since minimal surfaces are described by equations, computers can solve the equations and plot the results as pictures on a screen. Dr. Hoffman, with William H. Meeks 3d of Rice University and James T. Hoffman of the University of Massachusetts, did just that, moving between equations and their visual representations, letting the pictures suggest modifications to the equations.

In doing so, they discovered whole families of new minimal surfaces—weird shapes with holes and handles that had eluded the unaided mathematical imagination.

“The computer has taken the place of soap film experiments and allowed one to bring one’s visual and tactile sense to a problem that was mostly mathematical,” Dr. Hoffman said. “We then use the insight from the pictures to go back and produce a formal proof.”

Dr. Hoffman suggests that the use of computers brings mathematicians closer in spirit to practical scientists. He has been working with chemists who have now observed his surfaces in their experiments.

Whether computers will change the way mathematicians think of formal proof is a troublesome question. Several important proofs of the last few years have been so huge, thousands of pages, that the results could be assembled only with computers. Other kinds of proofs use computers for calculations that could, in theory, be performed by a human—but only in theory. Some calculations are just too complicated. Suppose a proof relies on the fact that 3 times 4 equals 12, asked Jean-Pierre Eckmann, a Swiss mathematician. Suppose further that

your calculating ability is so weak that you need a machine for the multiplication. Should that invalidate the proof?

For some, the most irksome problem is that proofs using computation lie beyond the reach of any one mathematician. "Traditionally, you like to think about a problem, and after a while it becomes all clear in your mind," said David Ruelle of the Institut des Hautes Études Scientifiques in France. "This sort of mathematics might die."

August 24, 1986

With Major Math Proof, Brute Computers Show Flash of Reasoning Power

By GINA KOLATA

Computers are whizzes when it comes to the grunt work of mathematics. But for creative and elegant solutions to hard mathematical problems, nothing has been able to beat the human mind. That is, perhaps, until now.

A computer program written by researchers at Argonne National Laboratory in Illinois has come up with a major mathematical proof that would have been called creative if a human had thought of it. In doing so, the computer has, for the first time, got a toehold into pure mathematics, a field described by its practitioners as more of an art form than a science. And the implications, some say, are profound, showing just how powerful computers can be at reasoning itself, at mimicking the flashes of logical insight or even genius that have characterized the best human minds.

Computers have found proofs of mathematical conjectures before, of course, but those conjectures were easy to prove. The difference this time is that the computer has solved a conjecture that stumped some of the best mathematicians for 60 years. And it did so with a program that was designed to reason, not to solve a specific problem. In that sense, the program is very different from chess-playing computer programs, for example, which are intended to solve just one problem: the moves of a chess game.

"It's a sign of power, of reasoning power," said Dr. Larry Wos, the supervisor of the computer reasoning project at Argonne. And with this result, obtained by a colleague, Dr. William McCune, he said, "We've taken a quantum leap forward."

Dr. Wos predicts that the result may mark the beginning of the end for mathematics research as it is now practiced, eventually freeing mathematicians to focus on discovering new conjectures, and leaving the proof to computers.

But the result also may challenge the very notion of creative thinking, raising the possibility that computers could take a parallel path to reach the same conclusions as great human thinkers. Or it may be that since no one has any idea how humans think, the magnificent bursts of creativity that spring apparently full blown from the minds of geniuses are actually a result of hidden, computer-like drudge work in the unconscious recesses of the brain.

Dr. Stanley Burris, a mathematician at the University of Waterloo in Canada, said that the result was "the first sort of real breakthrough in automated theorem proving," and that it did seem to be different in kind from what went before. It shows, he said, that "it's a very thin line between the mechanical and the creative and it may disappear."

Dr. Robert Boyer, a computer scientist at the University of Texas in Austin, hedged. "I think it's the most remarkable result in automated theorem proving in 30 years," he said, and "clearly a form of computer thinking." But, he added, "I don't want to make too much of that." It's best, he said, to think of a computer as "just another colleague, one that is sometimes helpful, but often not."

Dr. McCune's proof concerns a conjecture that is the very epitome of pure mathematics. "It has no applications," Dr. McCune said. His computer program proved that a set of three equations is equivalent to a Boolean algebra, that set of rules, familiar to generations of high school students, that govern unions and complements and intersections among sets.

The problem was first posed in the 1930s by Dr. Herbert Robbins, who is New Jersey Professor of Mathematics at Rutgers University in New Brunswick. Dr. Robbins said that he worked on the problem for some time, and then passed it on to one of the century's most famous logicians, Dr. Albert Tarski of Stanford University. Dr. Tarski, who is now dead, worked on the problem, included it in a book, and handed it out to graduate students and visitors.

Dr. Burris, for example, said that Dr. Tarski suggested the problem to him in the early 1970s, while he was visiting Stanford for a couple of months. Dr. Tarski, he said, "liked to throw out challenging problems to people passing through."

While mathematicians were batting around Dr. Robbins's problem, computer scientists were striving to see if they could get computers to reason. Among them was Dr. Wos, who started working on automated reasoning in the 1960s. It was a time when computers were primitive, clunky and slow, and researchers were divided on how to proceed. Some believed the key was to figure out how humans reasoned and then to create computer programs that mimicked the process. Dr. Wos disagreed.

"Nobody knows how humans reason," he said. "When you talk to mathematicians and say, 'I understand you proved a great theorem. How did you do it?' They'll say, 'Well, I walked around my house a lot and I read some papers and I thought.'"

So he and his colleagues followed a different path. "We didn't ask ourselves what people do when they think," Dr. Vos said. "That was irrelevant," he said. Instead, he said: "We asked how can you tell a computer what this problem is about? How can you get it to draw conclusions that follow inevitably and logically from hypotheses and thereby prove theorems?"

He and his colleagues began writing programs in which the computer would assume that the hypothesis in question was false and would then examine the consequences. If it found a contradiction, that would be proof that the hypothesis was true. The computer would also assume that the hypothesis was true and do the same thing, looking for contradictions that would show it was false.

To prevent the computer from getting lost in checking out lengthy chains of extended consequences, the investigators added strategies like ignoring any logical statements that contained more than 100 symbols.

"I got into strategy because I was a poker player and a bridge player," Dr. Vos said. "A good con man uses strategy. He figures out what your weakness is and plays to that weakness. He doesn't just randomly try to trick you."

Dr. Vos's computer programs were soon able to find proofs for basic mathematical problems. "We could do the problems sometimes better than the students and sometimes, once in a great while, better than the professors could," Dr. Vos said.

For more than 16 years, Dr. Vos and his colleagues stuck to problems from mathematics textbooks. Dr. Vos explained that when the computer tried to prove something for which a proof existed, and failed, the investigators knew that "there's a problem with our program." If they try to solve an unsolved problem, and fail, they have no way of knowing whether they missed something obvious.

"My own mathematician friends would say, 'Vos, why are you doing what we already know? Why don't you give us something new?'" Dr. Vos said. In the early 1970s, he said, he told one of his badgering friends that he thought it would be another 30, 40 or even 50 years before computers could solve major problems that had stumped mathematicians.

The first time they tried something new was in 1978, when Dr. Vos said, "a little baby problem" came along. They solved it, and then solved five others like it. Dr. Vos was ecstatic. "We had done more than I thought I could do in my lifetime," he said.

The group kept adding strategies to its programs. It added one recently that said to try things that worked in previous problems. Dr. Vos said some of his

colleagues scoffed at that and that he himself did not know if it would work. But, he said, it turned out to be surprisingly useful.

In 1979, Dr. Wos learned about Dr. Robbins's problem. Although he and his colleagues tried to solve it from time to time with ever more refined computer programs, they failed. Dr. McCune joined the group in 1984, with a new Ph.D. from Northwestern University and a thirst to see how far he could push computers.

The fact that the Robbins conjecture was certifiably hard—it had, after all, stumped some of the best minds in mathematics and had gone unsolved for decades—appealed to Dr. McCune. But the problem also thwarted his best computer reasoning programs.

Finally, on Oct. 2, Dr. McCune gave the Robbins conjecture to a new automated reasoning program that he had written called EQP, for equational prover. Eight days later, on Oct. 10, the computer spewed out a proof. Dr. McCune, a low-key researcher, said he was “amazed.” Dr. Wos, his exuberant supervisor, said, “Bill was in heaven.”

Encouraged, Dr. McCune tried to get the computer to refine the proof. He started his program searching for a better proof on Nov. 15. It found one on Nov. 25.

Dr. McCune said he had checked his proof by computer and by hand. Dr. Mark Stickel of the Stanford Research Institute in Palo Alto, Calif., independently checked it with his computer program. And Dr. Burris independently checked it by hand.

Dr. Burris said the proof, fresh from the computer, was in the form of statements so long that he had to print them sideways across the page, and he had to specify that the printer use small type. “It was pretty unreadable,” he said. “The machine says, ‘I got that step from two steps before,’ but it doesn’t fill in all the details.” He spent several days rewriting it and now has it down to three normal-looking pages of mathematical statements.

The proof will be published within a few months in *The Journal of Automated Reasoning*, Dr. Wos said. He will also put it on the Internet and will request more problems as certifiably hard as Dr. Robbins’s problem.

When he saw that he had actually proved Dr. Robbins’s conjecture, Dr. McCune called the 81-year-old mathematician at his office at Rutgers, amazing him with the news. In a telephone interview, Dr. Robbins said he was delighted. “Isn’t that marvelous,” he said. “I’m glad I lived long enough to see it.”

But Dr. McCune certainly had a different experience than a mathematician might have had if he or she had created the proof with pure thought. So was

something lost in the process? Did Dr. McCune have anything resembling a eureka moment?

Well, not quite, Dr. McCune said. "I have a good feeling," he said. "In a sense, I have a feeling that the computer has been creative."

Dr. McCune, however, said he had little interest in speculating on the philosophical implications of his work. "I just work on the problems and try to solve them," he said.

Not so Dr. Wos, who loves to ponder the meaning and future of human reasoning. After all, he said, he insisted on calling his computer project "automated reasoning," rather than "automated theorem proving," as some suggested, explaining that "it's not just mathematics that I care about."

Dr. Wos predicts that in a few decades computers might be as agile at reasoning as they now are at calculating.

Dr. Daniel Dennett, a philosopher who directs Tufts University's Center for Cognitive Studies, said, "Philosophers have often dreamt of such a device—a thought processor instead of a word processor.

"If you start inferring invalidly because you left out a premise, it will say, 'Wait a minute,'" he explained.

Dr. Wos said, "I want to tell people the real truth of it," adding, "If we succeed really big," giving people handheld thought processors like they now have handheld numerical calculators, "what an incredible improvement we can make to their lives."

December 10, 1996

Computers Still Can't Do Beautiful Mathematics

By GINA KOLATA

Mathematicians often say that their craft is as much an art as a science. But as more and more researchers are using computers to prove their theorems, some worry that the magic is in danger of fading away.

In the past, mathematicians could count on being able to sit down with a newly published proof and carefully follow the researcher's logic, determining whether the derivations held true, relishing particularly clean and clever arguments.

But when a computer is used to help prove a conjecture, reasoning is often replaced by calculation. Instead of converging on an answer through a long chain of logical deduction, mathematicians now often use computers to systematically test and discard a vast number of possible answers until they hit on the right one.

Dr. Daniel Kleitman, a mathematician at the Massachusetts Institute of Technology, explained why many mathematicians shrink back from this experimental approach. "One's motivation for reading a paper is not only to become aware of the results, but also to understand how such a proof is formulated and how it actually works," he said. "The question is, Do you want to have an experimental mathematics? Do you want to make traditional papers into experimental things?"

Many mathematicians object to being put in the position of having to trust a computer and the assumptions made by its programmer. In a sense, the program itself becomes a part of the proof, and few mathematicians are equipped to check its reliability.

In May Dr. Fan R. K. Chung, the editor of the *Journal of Graph Theory*, decided that she was getting so many computer-aided proofs that it was time to formulate a policy. She wrote to her 20-member editorial board, providing one newly received paper as a test case. "Is an important result with a computer-assisted proof acceptable?" she asked. If so, "how should the paper be evaluated knowing that it is almost impossible for the referee to verify its correctness?"

The paper that Dr. Chung chose as an example was submitted by Dr. Brendan McKay of the Australian National University and Dr. Stanislaw P. Radziszowski of the Rochester Institute of Technology. It solved a variant of what mathematicians call the party problem: What is the minimum number of people you have

to invite to a party to be sure that, among them, there are eight people or more who all know one another or three people or more who are all strangers to one another? The answer, discovered after some marathon computer crunching, is 28.

A classical proof would have demonstrated through an unassailable chain of logic that the answer could only be 28. Instead, Dr. McKay and Dr. Radziszowski took an experimental approach.

Even with a computer, it would be impossible to examine the myriad ways—10 followed by 112 zeros—that 28 party-goers could be acquainted with one another. But using some clever mathematics, Dr. McKay and Dr. Radziszowski cut down the number of calculations to a mere 100 trillion and then automatically sifted through permutation after permutation, ruling out all gatherings smaller than 28.

In the end, the method gave an answer, but did not show why the answer was what it was. And it could not be generalized to solve other party problems.

Computer-aided proofs have been a festering problem in mathematics for 14 years, ever since a famous conjecture, the four-color problem, was solved. The problem asked whether any arbitrary map of real or invented countries could be colored, as was generally believed, with four or fewer different colors. No two adjacent countries could be colored the same.

In 1977, Dr. Kenneth Appel and Dr. Wolfgang Haken of the University of Illinois published a paper proving that four colors were indeed enough. But the 100-page proof relied on extensive computer calculations. The mathematicians argued that all possible maps could be boiled down to 2,000 standard configurations and then proved, by trying different colorings, that each of those 2,000 maps could be colored in four or fewer hues.

"It was a very routine type of calculation that was just repetitive," Dr. Appel said.

Many mathematicians found the proof difficult to swallow. It revealed no deep mathematical truths and provided no techniques that could help with other problems.

"It is such a nasty situation," Dr. Chung said. "A lot of people just reject the proof outright. It goes against the instincts of most mathematicians."

In their replies to Dr. Chung, many members of her editorial board expressed their hesitation about embracing such proofs. Dr. Frank Harary of New Mexico State University wrote that the proof should be "fully verified as correct by an independent computing organization" before the journal considers it. Then, if it

accepts the paper, it should publish only the result, he said, while the proof should appear in a computer journal.

Dr. Gary Chartrand of Western Michigan University suggested that the result could be published in a special section, titled something like "Research Announcement," taking care to mention that the proof had not been verified. Several others, like Dr. Noga Alon of Tel Aviv University, suggested that the journal accept only papers on "important" theorems and then require the authors to submit a copy of their program, so it could be available to others if they wanted to examine it.

In the end Dr. Chung decided to accept the paper. But she decided not to ask for the program. "I don't think the journal should be held accountable," she said. "I think computer-aided proofs are a trend we cannot ignore. But we have to weigh them. If it is a computer-assisted proof, it is a minus. If it is a classical problem, it is a plus."

While computer-aided proofs may be published as mileposts on the way to solving a problem, many mathematicians won't consider the problem really solved until there is a proof—even if it is a hundred or more pages long—that a lone human sitting in a room can go through line by line and understand.

July 14, 1991

100 Quadrillion Calculations Later, Eureka!

By GINA KOLATA

An international effort to crack a tough mathematical problem has succeeded, researchers said yesterday. The problem has stood out as a challenge to computer scientists for 17 years because it was linked to a popular coding system and was said to be proof of the system's security.

The problem was to factor a 129-digit number, breaking it into its component parts the way a molecule is broken into atoms. This particular number was suggested 17 years ago by the inventors of a coding system that was said to be provably secure because to break it a person would have to factor a very large number.

To show how hard it was, the inventors of the coding system published the 129-digit number, encoded a message with it, and challenged people to break the code and read the message. They predicted that it would take 40 quadrillion years to factor it with the methods of the time and that no one would be able to break the code until well into the next century.

They offered \$100 to anyone who could factor the number.

The number was known as R.S.A. 129, for the last names of the coding system's inventors: Dr. Ronald Rivest of the Massachusetts Institute of Technology, Dr. Adi Shamir of the Weizmann Institute of Science in Rehovoth, Israel, and Dr. Leonard Adleman of the University of Southern California.

System Is Called Secure

Dr. Rivest, who knew that the factoring was imminent, said the solution to the problem did not mean that the coding system is not secure.

People typically use numbers that are 135 or 150 digits long when they use the coding system in banking, in the military and in protecting the security of nuclear power stations.

They could use larger numbers if they wished, although the numbers chosen now are ones that allow the code to fit on a single computer chip. Dr. Rivest said that with improvements in chip technology, those limits are being extended.

In the years since R.S.A. 129 was set out as a challenge, computers have got much faster and have been linked together in networks. In addition, mathematicians have found better ways to factor numbers. So, eight months ago, several

computer scientists proposed recruiting volunteers on the Internet, the international electronic mail system, to work together to crack R.S.A. 129.

Dr. Arjen Lenstra, a computer scientist at Bellcore in Morristown, N.J., said it took 100 quadrillion calculations, contributed by more than 600 Internet volunteers, to factor the number. Derek Atkins, a graduate student at the Massachusetts Institute of Technology, collected the calculations, checked them and passed them on to Dr. Lenstra. Dr. Lenstra used a Bellcore computer with 16,000 processors to churn out the factors of R.S.A. 129.

The answer, the group said, is this:

$$\begin{aligned} &114,381,625,757,888,867,669,235,779,976,146,612,010, \\ &218,296,721,242,362,562,561,842,935,706,935,245,733, \\ &897,830,597,123,563,958,705,058,989,075,147, 599, \\ &290,026,879,543,541 = 3,490,529,510,847,650,949,147, \\ &849,619,903,898,133,417,764,638,493,387,843,990,820, \\ &577 \times 32,769,132,993,266,709,549,961,988,190,834, \\ &461,413,177,642,967,992,942,539,798,288,533. \end{aligned}$$

The encoded message says: "The magic words are squeamish ossifrage."

Mr. Atkins said that the group is donating the \$100 reward to the Free Software Foundation, a group that distributes free computer programs.

Asked what he could do for an encore, Dr. Lenstra said he planned to factor other numbers much larger than anyone thought possible, using a new method he is developing. But he would not disclose the number he will try to solve next. He said he would leave that as a surprise for Dr. Rivest, whose company sells the coding system.

April 27, 1994

Theorist Applies Computer Power to Uncertainty in Statistics

By GINA KOLATA

A new technique that involves powerful computer calculations is greatly enhancing the statistical analysis of problems in virtually all fields of science.

The method, which is now surging into practical use after a decade of refinement, allows statisticians to determine more accurately the reliability of data analysis in subjects ranging from politics to medicine to particle physics.

The technique also enables statisticians to pull more information out of data than any statistical method previously developed, making it possible to solve some problems that had proved intractable, leading statisticians say. The method addresses the key problem in statistics: how to infer the truth from a sample of data that is by no means complete.

"There's no question but that it's very, very important," said Frederick Mosteller, a statistician at Harvard University. Because the method replaces standard, and simplifying, assumptions about data with extensive computer calculations, it can be a powerful tool, Dr. Mosteller said.

"It gives us another way to get empirical information in circumstances that almost defy mathematical analysis," he said. "It's a nice way of letting the data speak almost for themselves."

Jerome H. Friedman, a Stanford statistician who has used the new method, called it "the most important new idea in statistics in the last 20 years, and probably the last 50." He added, "Eventually, it will take over the field, I think."

The new method was invented in 1977 by Bradley Efron, a statistician at Stanford University, to take advantage of the high-speed power of computers. Conventional statistical methods were developed for the most part between 1800 and 1930, when computation was slow.

The standard methods were therefore forced to rely on statistical measures that can easily be calculated by mathematical equations. In contrast, the new method uses the number-crunching power of computers to perform statistical analyses that lie beyond the reach of mathematical equations but can be dealt with through millions of numerical calculations.

"If statistics had evolved at a time when computers existed, it wouldn't be what it is today," Dr. Efron.

The old and the new methods are both designed to determine how accurately a sample of data, such as people who are asked whom they will vote for, represents the whole array of possible data.

For example, a national survey typically draws a sample of 500 to 1,000 people, Dr. Friedman said. The hope is that the group is representative of the population, but in fact it is only a small sample of 150 million people. The basic question of statistics is, if a different group of voters had been selected, would the survey results come out the same?

The conventional method determines the accuracy of a sample by comparing it, in a theoretical exercise, with additional hypothetical samples that are generated mathematically. These artificial samples are based on the assumption that all the data fall into a "normal distribution" that conforms to a bell-shaped curve, with a few low values, a few high values, and a great mass of middle values.

Dr. Efron's new method allows statisticians to construct artificial data sets without making any assumptions about bell-shaped curves.

Instead, the computer constructs new data sets by randomly picking data from the original set.

If the data set were 10 measurements of the effect of a new drug on high blood pressure, these 10 measurements would be entered into the computer. The computer would randomly pick a measurement from among the 10 and use that number to start a new data set while leaving it as well in the original data set. In the same way, the computer would pick a second number, a third, and so on until it had picked ten numbers for the first set of artificial data. The computer could repeat this process 100 times, for example, creating 100 new data sets. In each data set, some of the original 10 numbers could, by chance, be chosen more than once and others might not be chosen at all.

Simple but Powerful

By analyzing how these data sets vary from the original one, statisticians can determine the reliability of the inference they drew from the original 10 numbers. The method, conceptually simpler than the conventional methods, requires too many calculations to be done without a computer.

Dr. Efron calls his method "the bootstrap" because the data, in a sense, pull themselves up by their own bootstraps by generating new data sets through which

their reliability can be determined. His method is the most prominent of several that rely on the power of computers to generate artificial data sets. Persi Diaconis, a statistician at Harvard University, said Dr. Efron's technique is "very simple but remarkably powerful." He added, "You can use it across a broad spectrum of problems."

The method is now coming into practical use, after having been argued and discussed by theoretical statisticians for several years.

"It was a practical idea, but it went through a big theoretical development with statisticians tearing it in a whole bunch of directions," Dr. Diaconis said. "Now there has been a synthesis and it boils down to simple recommendations on how to use it in the most sensible way in day-to-day situations."

Dr. Efron said new users of the method include paleontologists, physicists, economists and psychometricians, who study the results of psychological testing.

Dr. Efron's idea allows statisticians to use unorthodox methods to see patterns in data because now, for the first time, statisticians can assess how accurate those methods are.

When the Curve Isn't Correct

In recent studies applying his method to data collected by others, Dr. Efron has found that a cholesterol-lowering drug may be more effective than previously suspected and that a subatomic particle may decay in an unexplained way.

In some cases, the bell-shaped curve assumption of classical statistics is correct, and then the bootstrap method gives the same answer as the standard methods. But Dr. Friedman said, "Data don't always follow bell-shaped curves, and when they don't, you make a mistake" with the standard methods. In fact, he added, the data frequently are distributed quite differently than in bell-shaped curves, although "no one knows" how often this occurs.

Using the new method, Dr. Efron recently analyzed data on the decay of tau particles, which are produced in particle accelerators and studied by physicists who want to understand the fundamental nature of matter. The data were supplied to him by Martin L. Perl, a Stanford physicist, who was puzzled by the traditional statistical analysis, which indicated that there might be a mysterious new way that the particles could decay.

The new analysis gave a more precise estimate of the accuracy of the physics data and indicated more firmly that some decay of the tau particles is not explained

by the traditional theories, Dr. Efron found. He added that the new analysis gave more definitive, and believable, evidence to the theoretical physicists.

Analyzing Drug Dosage

In another recent study, Dr. Efron obtained data from a study of cholestyramine, a cholesterol-lowering drug, from Dr. John Farquhar and Dr. Daniel Feldman of Stanford Medical School. The data were from a clinical trial sponsored by the National Heart, Lung and Blood Institute more than a decade ago. The data showed that the more cholestyramine the patients took, up to the maximum daily dose, the more their blood cholesterol dropped. The standard method of analysis indicates that there is a straight-line relationship between the amount of cholestyramine a patient takes and the amount the blood cholesterol is lowered.

But a different way of analyzing the data seemed to give a more accurate picture, Dr. Efron found. The reliability of that method could be assessed only by the new method. The new analysis indicated that when patients took more of the drug they did better than what would have been expected by the straight-line relationship.

November 8, 1988



CHAPTER 2

Statistics, Coincidences and Surprising Facts

HOW MANY TIMES DO YOU HAVE TO SHUFFLE CARDS, imperfectly, to perfectly mix a deck? The answer turns out to be seven. The cards will be in random order with only seven shuffles. And while that may seem to be an esoteric fact—it turns out that it took sophisticated math to prove it—some card players, instinctively realizing that dealers do not generally shuffle enough, make money on the non-randomness of most shuffles.

Mathematics and statistics sometimes address problems like shuffling, partly for fun and partly because the researchers have particular interests. The statistician who solved the shuffling problem, Persi Diaconis, is also a magician.

Their findings can be startling. It turns out that there actually is no precise way to know such things as the number of people who live in the United States or the number of unemployed. That is why recounts, like the ones in Florida in the 2000 presidential race, could never really settle the issue of who won, Bush or Gore, even though the Supreme Court eventually weighed in and declared George W. Bush the winner.

Others can have practical implications. One way to make traffic flow more freely, it turns out, is to actually close some streets. Mathematicians can prove it, although planners may not believe it. As for evaluating teachers with exact numbers that reveal how successful they are, well, a commentary titled "Metric Mania" tells all you may need to know.

1-in-a-Trillion Coincidence, You Say? Not Really, Experts Find

By GINA KOLATA

Coincidences, those surprising and often eerie events that add spice to everyday life, may not be so unusual after all, researchers say.

After spending 10 years collecting thousands of stories of coincidences and analyzing them, two Harvard statisticians report that virtually all coincidences can be explained by some simple rules.

Some of the analyses performed by them or other statisticians showed that events that looked extremely unlikely were almost to be expected. When a woman won the New Jersey Lottery twice in four months, the event was widely reported as an amazing coincidence that beat odds of 1 in 17 trillion. But when carefully analyzed, it turned out that the chance that such an event could happen to someone somewhere in the United States was more like 1 in 30.

It was an example of what the authors, Dr. Persi Diaconis, a professor of mathematics at Harvard University, and Dr. Frederick Mosteller, an emeritus mathematics professor at Harvard, call "the law of very large numbers." That long-understood law of statistics states, in their formulation: "With a large enough sample, any outrageous thing is apt to happen."

Some of the findings are published in the December issue of the *Journal of the American Statistical Association*; others are now appearing in other professional journals. Dr. Diaconis, whose work also led to the recent discovery that seven shuffles are needed to mix a 52-card deck randomly, said the findings on coincidence were meeting mixed reactions. "Some people are enormously relieved, but others are furious," he said. Not everyone who supplied an amazing coincidence to the researchers wanted to hear that a cherished dramatic story was really nothing special.

"I think the whole subject is fascinating," said Dr. Erich Lehmann, a statistician at the University of California at Berkeley. Although it can be a difficult statistical problem to decide just how unlikely an event is, Dr. Lehmann said, there is no dispute about the validity of the findings of Dr. Diaconis and Dr. Mosteller, some of which have been discussed at statistical meetings in recent years.

The two Harvard statisticians reviewed a large body of calculations and analyses of coincidences performed by other researchers, and they devised new

techniques and approaches for studying the phenomenon in a wide range of circumstances. The research results, Dr. Diaconis said, "are aimed at very basic problems of inference that arise in messy, real statistical problems."

Dr. Bradley Efron, a statistician at Stanford University, said coincidences arise "all the time" in statistical work. When researchers find clusters of odd cancers or birth defects or other diseases, statisticians are asked "to decide which events are the luck of the draw" and which may reflect some underlying cause, Dr. Efron said. "That's what Persi and Fred are trying to unravel," he added. "I think it's a very interesting enterprise."

Dr. Diaconis said one application of the new analyses is in scrutinizing data from clinical trials of new drugs. "As you are looking around in that mass of data," he said, "you find that in a certain subgroup, there are twice as many deaths in people taking drug A as there are in people taking drug B." Is it a coincidence or an indication that drug A is so dangerous to some patients that the trial must be stopped?

Dr. Diaconis and Dr. Mosteller said they decided to study coincidences because they were fascinated by the role these odd events play in everyone's lives. "All of us feel that our lives are driven by coincidences," Dr. Diaconis said. "Who we live with and where we work, why we do the things we do often rest on slim coincidences." These chance events "touch us very deeply," he said. The two statisticians defined a coincidence as "a surprising concurrence of events, perceived as meaningfully related, with no apparent causal connection."

Dr. Diaconis and Dr. Mosteller began with the presumption that there are no extraordinary forces outside the realm of science that are acting to produce coincidences. But they also recognized that seeming coincidences are an important source of insight in science and so should not be dismissed out of hand. What looks like a coincidence may in fact have a hidden cause, which can lead to a new understanding of a phenomenon. A sequence of odd blips on a chart, a clustering of cases of a rare disease can tell researchers that a new event is occurring.

Anthologies of Happenstance

A decade ago, Dr. Diaconis and Dr. Mosteller started asking their colleagues, friends and friends of friends to send them examples of surprising coincidences. The collection quickly mushroomed. Dr. Mosteller said he had 13 notebooks, each three and a half inches thick, full of coincidences. "These notebooks are

eating up the shelves in my den," he said. Dr. Diaconis said he had 200 file folders full of coincidences.

When they began to study these coincidences, they learned that they fell into a several distinct groups. Some coincidences have hidden causes and are thus not really coincidences at all. Others arise from psychological factors, like selective memory or sensitivities, that make people think particular events are unusual whether they are or not. But many coincidences are simply chance events that turn out to be far more likely statistically than most people imagine. The analyses often required the researchers to develop new statistical methods, but in the end almost all coincidences could be analyzed.

The law of truly large numbers, which explains the double winner of the New Jersey Lottery, says that even if there is only a one-in-a-million chance that something will happen, it will happen eventually given enough time or enough people. "It's the blade-of-grass paradox," Dr. Diaconis said. "Suppose I'm standing in a large field and I put my finger on a blade of grass. The chance that I would choose that particular blade may be one in a million. But it is certain that I will choose a blade." So if something happens to only one in a million people per day and the population of the United States is 250 million, "you expect 250 amazing coincidences every day."

"If a one-in-a-million thing happens to you, you start telling people about it," Dr. Diaconis went on. "You might say to me, 'So what do you think of that, wise guy?' And I say, 'It's an example of the law of truly large numbers.'"

Right Answer, Wrong Question

When a New Jersey woman won the lottery twice in a four-month period, it was reported as a 1-in-17-trillion long shot. Narrowly speaking, that is correct. But as Dr. Diaconis and Dr. Mosteller reported, 1 in 17 trillion is the odds that a given person who buys a single ticket for exactly two New Jersey lotteries will win both times. The true question, they say, is, "What is the chance that some person, out of all the millions and millions of people who buy lottery tickets in the United States, hits a lottery twice in a lifetime?"

That event was called "practically a sure thing" by Dr. Stephen Samuels and Dr. George McCabe, two statisticians at Purdue University. Over a seven-year period, they concluded, the odds are better than even that there will be a double lottery winner somewhere in the United States. Even over a four-month

period, the odds of a double winner somewhere in the country are better than 1 in 30.

Another principle that demystifies many coincidences is what the researchers call "multiple end points"—occasions when what might qualify as a coincidence is not spelled out ahead of time, and when many chance events would qualify. This could apply, for example, at a party, where two people might discover that they come from the same town. This may seem a surprising coincidence. But the truth is that almost anything two strangers have in common would count as a coincidence—the same first or last name, the same birthday, the same item of clothing.

"Clearly, the chances of getting a match in any of several things is bigger than if you look at just one thing," Dr. Diaconis said. He and Dr. Mosteller have developed a formula that can evaluate such problems.

Multiple end-point coincidences often sound amazing on the surface. For example, Dr. Diaconis said, "I had a friend who said, 'Gee, I was watching a James Bond movie and there was a four-digit code on a bomb that was exactly the same as the code on my Israeli bank account.'" It sounded extraordinary, since there are 10,000 possible four-digit numbers. But Dr. Diaconis went on: "If you know 120 numbers—Social Security numbers, bank codes, telephone numbers of friends—there are even odds that four digits of two of them will match," he said.

A third category of coincidences is those that are close but not exact. The odds of a coincidence then go up enormously. Once again, the two Harvard statisticians have developed a formula to analyze these problems.

Birthdays and Near Birthdays

For example, with 23 people in a room, the chances are even that two of them will have the same birthday. But with only 14, there is an even chance of finding two people born within a day of each other, and if you ask instead that the birthdays match within a week, you need only seven people.

"I have a friend who said, 'My daughter, myself, and my husband all have a birthday on the 11th of a month,'" Dr. Diaconis recalled. "O.K., there are 30 categories, 30 days of the month. How many birthdays do we have to know so that three are on the same day of the month?" The answer, he calculated, is 18. "So if you know 18 people, it's even odds that three will be born on the same day of the month," he explained. So the friend's birthday coincidence, he said, "is not so unusual."

By analyzing coincidences with these three principles in mind, Dr. Diaconis and Dr. Mosteller find that what looks unexpected usually turns out to be expected. No strange forces outside the realm of science are needed to explain coincidences.

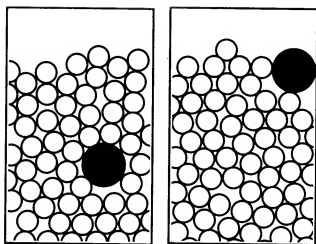
“Why does an educated person think there might really be something in coincidences?” Dr. Diaconis asked, and answered his own question: “No one story holds up on its own. But taken together, they mean something.” If you put all these near coincidences together, doesn’t it indicate that something strange is going on?

It does not, Dr. Diaconis replied, and quoted another fundamental law of logic: “A lot of flawed arguments don’t produce a sound conclusion.”

February 27, 1990

Sometimes Heavier Objects Go to the Top: Here's Why

By JAMES GLEICK



Physics—the same enterprise that regularly predicts the emergence of bosons and mesons from high-energy particle collisions—has been unable until now to explain why the brazil nuts rise to the top of a jar of mixed nuts. But that barrier seems finally to have fallen.

Scientists have long known that in any mixture of large and small objects, the large ones tend to go up while the small ones go down. Oddly, the effect occurs even when the large objects are heavier and denser.

Using a combination of theory and computer simulation, a team of physicists and engineers at Carnegie Mellon University in Pittsburgh has come up with a model that appears to explain why. Their findings affect metallurgy, concrete, pharmaceuticals and a host of other industries that try to mix powders by shaking them, only to find, all too often, that the powders separate instead.

Beyond the practicalities, the model addresses an ancient fact of nature: one reason, for example, that heavy rocks continue to rise to the surface of soil that farmers have cleared for generations.

"They will keep on doing that as long as the earth exists," said Friedrich Prinz of Carnegie Mellon. "And if you eat corn flakes, as you know, you eat the big corn flakes for the first few days, and then you eat the junk."

Dr. Prinz and his colleagues—Anthony Rosato, Katherine J. Strandburg and Robert H. Swendsen—report their brazil-nut theory in *Physical Review Letters*, just after a paper titled "Electronically Driven Instabilities and Superconductivity in the Layered $\text{La}_{2-x}\text{Ba}_x\text{CuO}_4$ Perovskites" and before one titled "Electromagnetic Radiation from Superconducting Cosmic Strings." They are not at all embarrassed to be in such company.

"It's one of these things that's obvious after it's been explained, but there is still some controversy about it," said Dr. Swendsen, a Carnegie Mellon physicist. "It's really a very serious engineering problem. This segregation effect occurs all over in applications."

Their goal was to take a process that many engineers felt they understood in a seat-of-the-pants way and to develop a more scientific understanding, offering a theory that makes specific predictions to be tested with a computer model.

Their solution reflects a growing tendency in physics to simulate seemingly complicated problems by throwing away many physical details. Early attempts to model the size-segregation phenomenon, either with equations or on computers, tried to give a realistic role to effects that included friction, the weight of the particles and their speed of rotation.

Some theorists have tried to think in terms of complicated blendings of centrifugal force and exotic acceleration effects in the equations that would model the millions of collisions of shaken objects.

The Carnegie Mellon group decided to ignore such things, noting that unmixing occurs consistently and universally, from powders to nuts. The process does not seem to care what the particular shape or roughness or weight of the objects are.

In their model, randomness is an essential element: particles just bounce around, colliding with one another and heading off in new directions, but not necessarily following trajectories with the sort of realism that a rocket scientist would expect.

They do not bounce around endlessly, though. As in real problems, each time the simulated container is given a shake, the particles bounce a little, lose energy and settle back down again. The shaking is repeated over and over again.

Shaking Opens Up Gaps

As the particles bounce upward, gaps open up beneath them—some large and some small. Small gaps, it turns out, are much more common than large gaps. As the particles fall, a small particle can move down into either a large or small gap, while a large particle can only move down if many small particles happen to have bounced out of the way.

That happens, but not often. So over time, the small particles tend to head downward and the large particles upward—by default.

Whether that seems childishly self-evident or physically implausible seems to depend on one's perspective. But it even happens when the large particles weigh considerably more. "It's kind of counterintuitive," Dr. Prinz said. "You wouldn't expect it from an energetic point of view."

In terms of energy, scientists expect systems to seek an equilibrium in which heavy things are at the bottom. That is the state in which a system's total potential energy is said to be smallest, and it is no different when the system is a can of nuts or balls.

But there is nothing sacred about thermodynamic equilibrium, as various industries have discovered after transporting mixtures in trucks or trains. Shaking mixes, but it also unmixes.

The industry whose problems most immediately motivated the Carnegie Mellon work is metallurgy. For many kinds of alloys, conventional casting by melting metals into liquid form is being replaced by a technology that starts with powders. The powder technology allows engineers to control the microscopic structure of the final product—a drill bit, say—by freezing in structures that are unstable at high temperatures.

Sometimes metallurgists use ultrasonic waves to turn the powder mixtures into compact solids. That is when they find that the shaking unmixes the powders.

The new theory may help suggest ways of avoiding the problem. For example, the computer simulations show that side-to-side shaking, as opposed to up-and-down shaking, does not cause the unmixing. In the meantime, it is helping the scientists understand a phenomenon that they now see everywhere they look.

Quarters Rise to Top

Dr. Strandburg, for example, noticed a container of different sized paper clips in which the large clips were mostly on top. A friend of hers, even when unapprised of the fundamental physics, has long used shaking to get quarters to the top of the can of change on his dresser.

"If you look in a flour sifter while you sift," she said, "things are bouncing around and large things tend to come up to the top."

To Dr. Strandburg, the simplicity of the solution is its beauty. "That's exactly the kind of thing that physicists look for in a scientific explanation," she said. "What you want to have is something that, when you hear it, you say, 'Oh, of course, why didn't I think of that?'"

March 24, 1987

Behind Monty Hall's Doors: Puzzle, Debate and Answer?

By JOHN TIERNEY

Perhaps it was only an illusion, but for a moment here it seemed that an end might be in sight to the debate raging among mathematicians, readers of *Parade* magazine and fans of the television game show *Let's Make a Deal*.

They began arguing last September after Marilyn vos Savant published a puzzle in *Parade*. As readers of her "Ask Marilyn" column are reminded each week, Ms. vos Savant is listed in the Guinness Book of World Records Hall of Fame for "Highest I.Q.," but that credential did not impress the public when she answered this question from a reader:

"Suppose you're on a game show, and you're given the choice of three doors: Behind one door is a car; behind the others, goats. You pick a door, say No. 1, and the host, who knows what's behind the other doors, opens another door, say No. 3, which has a goat. He then says to you, 'Do you want to pick door No. 2?' Is it to your advantage to take the switch?"

Since she gave her answer, Ms. vos Savant estimates she has received 10,000 letters, the great majority disagreeing with her. The most vehement criticism has come from mathematicians and scientists, who have alternated between gloating at her ("You are the goat!") and lamenting the nation's innumeracy.

Her answer—that the contestant should switch doors—has been debated in the halls of the Central Intelligence Agency and the barracks of fighter pilots in the Persian Gulf. It has been analyzed by mathematicians at the Massachusetts Institute of Technology and computer programmers at Los Alamos National Laboratory in New Mexico. It has been tested in classes from second grade to graduate level at more than 1,000 schools across the country.

But it was not until Thursday afternoon that a truly realistic simulation of the problem was conducted. The experiment took place at the Beverly Hills home of Monty Hall, the host of 4,500 programs of *Let's Make a Deal* from 1963 to 1990. In his dining room Mr. Hall put three miniature cardboard doors on a table and represented the car with an ignition key. The goats were played by a package of raisins and a roll of Life Savers.

After Mr. Hall allowed this contestant 30 independent attempts to win the car, two conclusions seemed clear: Ms. vos Savant's vitriolic critics, including

the mathematics professors, are dead wrong. But Ms. vos Savant is not entirely correct either, because there is a small flaw in her wording of the problem that was detected not only by Mr. Hall but also by some of the experts. Despite her impressive analysis and 228-point I.Q., she was not as quick as Mr. Hall in understanding the psychological dimensions of the problem.

“So Easy” to Blunder

A few mathematicians were familiar with the puzzle long before Ms. vos Savant's column. They called it the Monty Hall Problem—the title of an analysis in the journal *American Statistician* in 1976—or sometimes Monty's Dilemma or the Monty Hall Paradox.

An earlier version, the Three Prisoner Problem, was analyzed in 1959 by Martin Gardner in the journal *Scientific American*. He called it “a wonderfully confusing little problem” and presciently noted that “in no other branch of mathematics is it so easy for experts to blunder as in probability theory.”

The experts responded in force to Ms. vos Savant's column. Of the critical letters she received, close to 1,000 carried signatures with Ph.D.'s, and many were on letterheads of mathematics and science departments.

“Our math department had a good, self-righteous laugh at your expense,” wrote Mary Jane Still, a professor at Palm Beach Junior College. Robert Sachs, a professor of mathematics at George Mason University in Fairfax, Va., expressed the prevailing view that there was no reason to switch doors.

“You blew it!” he wrote. “Let me explain: If one door is shown to be a loser, that information changes the probability of either remaining choice—neither of which has any reason to be more likely—to $1/2$. As a professional mathematician, I'm very concerned with the general public's lack of mathematical skills. Please help by confessing your error and, in the future, being more careful.”

The criticism has continued despite several more columns by Ms. vos Savant defending her choice. “You are utterly incorrect,” insisted E. Ray Bobo, a professor of mathematics at Georgetown University. “How many irate mathematicians are needed to get you to change your mind?”

"The Henry James Treatment"

Mr. Hall said he was not surprised at the experts' insistence that the probability was 1 out of 2. "That's the same assumption contestants would make on the show after I showed them there was nothing behind one door," he said. "They'd think the odds on their door had now gone up to 1 in 2, so they hated to give up the door no matter how much money I offered. By opening that door we were applying pressure. We called it the Henry James treatment. It was 'The Turn of the Screw.'"

Mr. Hall said he realized the contestants were wrong, because the odds on Door 1 were still only 1 in 3 even after he opened another door. Since the only other place the car could be was behind Door 2, the odds on that door must now be 2 in 3.

Sitting at the dining room table, Mr. Hall quickly conducted 10 rounds of the game as this contestant tried the non-switching strategy. The result was four cars and six goats. Then for the next 10 rounds the contestant tried switching doors, and there was a dramatic improvement: eight cars and two goats. A pattern was emerging.

"So her answer's right: you should switch," Mr. Hall said, reaching the same conclusion as the tens of thousands of students who conducted similar experiments at Ms. vos Savant's suggestion. That conclusion was also reached eventually by many of her critics in academia, although most did not bother to write letters of retraction. Dr. Sachs, whose letter was published in her column, was one of the few with the grace to concede his mistake.

"I wrote her another letter," Dr. Sachs said last week, "telling her that after removing my foot from my mouth I'm now eating humble pie. I vowed as penance to answer all the people who wrote to castigate me. It's been an intense professional embarrassment."

Manipulating a Choice

Actually, many of Dr. Sachs's professional colleagues are sympathetic. Persi Diaconis, a former professional magician who is now a Harvard University professor specializing in probability and statistics, said there was no disgrace in getting this one wrong.

"I can't remember what my first reaction to it was," he said, "because I've known about it for so many years. I'm one of the many people who have written

papers about it. But I do know that my first reaction has been wrong time after time on similar problems. Our brains are just not wired to do probability problems very well, so I'm not surprised there were mistakes."

After the 20 trials at the dining room table, the problem also captured Mr. Hall's imagination. He picked up a copy of Ms. vos Savant's original column, read it carefully, saw a loophole and then suggested more trials.

On the first, the contestant picked Door 1.

"That's too bad," Mr. Hall said, opening Door 1. "You've won a goat."

"But you didn't open another door yet or give me a chance to switch."

"Where does it say I have to let you switch every time? I'm the master of the show. Here, try it again."

On the second trial, the contestant again picked Door 1. Mr. Hall opened Door 3, revealing a goat. The contestant was about to switch to Door 2 when Mr. Hall pulled out a roll of bills.

"You're sure you want Door No. 2?" he asked. "Before I show you what's behind that door, I will give you \$3,000 in cash not to switch to it."

"I'll switch to it."

"Three thousand dollars," Mr. Hall repeated, shifting into his famous cadence. "Cash. Cash money. It could be a car, but it could be a goat. Four thousand."

"I'll try the door."

"Forty-five hundred. Forty-seven. Forty-eight. My last offer: Five thousand dollars."

"Let's open the door."

"You just ended up with a goat," he said, opening the door.

The Problem with the Problem

Mr. Hall continued: "Now do you see what happened there? The higher I got, the more you thought the car was behind Door 2. I wanted to con you into switching there, because I knew the car was behind 1. That's the kind of thing I can do when I'm in control of the game. You may think you have probability going for you when you follow the answer in her column, but there's the psychological factor to consider."

He proceeded to prove his case by winning the next eight rounds. Whenever the contestant began with the wrong door, Mr. Hall promptly opened it and awarded the goat; whenever the contestant started out with the right door, Mr.

Hall allowed him to switch doors and get another goat. The only way to win a car would have been to disregard Ms. vos Savant's advice and stick with the original door.

Was Mr. Hall cheating? Not according to the rules of the show, because he did have the option of not offering the switch, and he usually did not offer it.

And although Mr. Hall might have been violating the spirit of Ms. vos Savant's problem, he was not violating its letter. Dr. Diaconis and Mr. Gardner both noticed the same loophole when they compared Ms. vos Savant's wording of the problem with the versions they had analyzed in their articles.

"The problem is not well-formed," Mr. Gardner said, "unless it makes clear that the host must always open an empty door and offer the switch. Otherwise, if the host is malevolent, he may open another door only when it's to his advantage to let the player switch, and the probability of being right by switching could be as low as zero." Mr. Gardner said the ambiguity could be eliminated if the host promised ahead of time to open another door and then offer a switch.

Ms. vos Savant acknowledged that the ambiguity did exist in her original statement. She said it was a minor assumption that should have been made obvious by her subsequent analyses, and that did not excuse her professorial critics. "I wouldn't have minded if they had raised that objection," she said Friday, "because it would mean they really understood the problem. But they never got beyond their first mistaken impression. That's what dismayed me."

Still, because of the ambiguity in the wording, it is impossible to solve the problem as stated through mathematical reasoning. "The strict argument," Dr. Diaconis said, "would be that the question cannot be answered without knowing the motivation of the host."

Which means, of course, that the only person who can answer this version of the Monty Hall Problem is Monty Hall himself. Here is what should be the last word on the subject: "If the host is required to open a door all the time and offer you a switch, then you should take the switch," he said. "But if he has the choice whether to allow a switch or not, beware. Caveat emptor. It all depends on his mood.

"My only advice is, if you can get me to offer you \$5,000 not to open the door, take the money and go home."

July 21, 1991

What If They Closed 42d Street and Nobody Noticed?

By GINA KOLATA

On Earth Day this year, New York City's Transportation Commissioner decided to close 42d Street, which, as every New Yorker knows, is always congested. "Many predicted it would be doomsday," said the Commissioner, Lucius J. Riccio. "You didn't need to be a rocket scientist or have a sophisticated computer queuing model to see that this could have been a major problem."

But to everyone's surprise, Earth Day generated no historic traffic jam. Traffic flow actually improved when 42d Street was closed.

To mathematicians, this may be a real-world example of Braess's paradox, a statistical theorem that holds that when a network of streets is already jammed with vehicles, adding a new street can make traffic flow even more slowly.

Seeking Out a New Street

The reason is that in crowded conditions, drivers will pile into a new street, clogging both it and the streets that provide access to it. By the same token, removing a major thoroughfare may actually ease congestion on the streets that normally provide access to it. And because other major streets are already overcrowded, diverting still more traffic to them may not make much difference.

Dr. Joel E. Cohen, a mathematician at Rockefeller University in New York, says the paradox does not always hold; each traffic network must be analyzed on its own. When a network is not congested, adding a new street will indeed make things better. But in the case of congested networks, adding a new street probably makes things worse at least half the time, mathematicians say.

Dr. Cohen and Dr. Frank P. Kelly of the University of Cambridge in England published the most recent analysis of the traffic paradox in the current issue of the *Journal of Applied Probability*. In their paper, they show that the paradox occurs when the traffic is described by a sophisticated statistical model. Previous work had used what Dr. Cohen describes as an overly simple and less realistic model.

The traffic paradox was first described in 1968 by Dr. Dietrich Braess of the Institute for Numerical and Applied Mathematics in Munster, Germany. He

found that when one street was added to a simple four-street network, all the vehicles took longer to get through.

Dr. Braess's result was "very surprising," said Dr. Richard Steinberg of A.T.&T.'s Bell Laboratories in Holmdel, N.J. Dr. Steinberg and colleagues studied how often the paradox would hold true, and determined in 1983 that "it is just as likely to occur as not."

He and his colleagues also turned up a paradox of their own: that in some situations, "when you add more delays along a route, more people use it."

Honk, Honk

Dr. Cohen and Dr. Kelly have now examined traffic networks with a sophisticated analytic method known as queuing theory, which describes traffic jams in terms of vehicles lining up on the streets. They found a simple traffic network in which adding a street increased travel time.

Their model starts with a V-shaped divide in the street, forcing drivers to go right or left. Those who bear left soon come to a garbage truck blocking one lane, and cars squeeze into a single lane to get by it. Ahead is a traffic light, which creates more delays. Finally, cars pass through the light and leave the network. Cars that bear right at the V face a traffic light and then some road construction that forces them into a single lane.

Now, Dr. Cohen and Dr. Kelly say, suppose a traffic engineer tries to improve things and adds a new street, from the garbage truck on the left to the construction on the right. The new street has its own traffic light in the middle. The addition of this connecting street, they find, slows everyone down by nearly 50 percent.

Everybody Gets Selfish

Dr. Cohen said he had not done a formal analysis to see how often additional streets clog traffic, but he added, "My intuition is that it must happen a lot." He finds support for his intuition from game theory, which says that if everyone in a game acts selfishly, everyone suffers. The traffic jam is analogous to such a game, Dr. Cohen said.

He cited a German paper, published in 1969, reporting that the City of Stuttgart had tried to ease downtown traffic by adding a new street. But congestion

only got worse, and so, in desperation, the authorities closed the street. Traffic flow improved.

New York's Transportation Commissioner, Mr. Riccio, has a doctoral degree himself (in engineering, from Lehigh University), and he said he favored using mathematical models to try to improve traffic flow. "I believe in these models," he said, and added that he would welcome a call from Dr. Cohen to discuss how his work could apply to New York City's daunting traffic problems.

December 25, 1990

Down for the Count; Why Some Numbers Are Only Very Good Guesses

By GINA KOLATA



Society runs on numbers: the number of people residing in the United States, the number of people in Florida who voted for each of the presidential candidates, the number of unemployed, the percent chance of a crippling blizzard.

Those who come up with these all-important digits know they aren't perfect, even if it sometimes comes as a surprise to the public. And some diehard believers in progress cling to the hope that technology will fix our numbers problem.

But some numbers just can't be fixed.

In some cases, the expectation of endless improvement has faltered before the Law of Unintended Consequences. What looks like a slick solution to a technical problem can introduce new problems, sometimes just as bad as the original ones. Instead of getting a better number, the result is a different number, with its own inaccuracies.

The census is a case in point. The Census Bureau's own estimates show that 3.3 million Americans were missed in its count for 2000. So why not use science—statistical adjustments—to put them back in?

An expert panel of the Census Bureau recommended that the census not be adjusted, but its decision neatly sidestepped Democratic arguments about its failure to fully count minorities and poor people and Republican defenses that the Constitution calls for an "actual enumeration."

The panel's reasoning: it could not conclude that an adjustment would bring the census any closer to the truth.

The commerce secretary, Donald L. Evans, said he relied on the panel's conclusion in deciding last week that unadjusted census figures would be used to draw up Congressional districts and distribute federal money to the states.

The reason it is hard to make the census more accurate is because methodological improvements have already lifted accuracy nearly as high as it seems able to go, said David Freedman, a statistics professor at the University of California at Berkeley.

In 1990, the national population count was 98 to 99 percent accurate, he said, and in 2000 it was even better. To improve further, scientists have to work within the remaining margin of error, using statistical methods to get better estimates of the number of people who were not counted, but should have been, and those who were counted, but should not have been.

"What they do is take a sample of 25,000 blocks sprinkled around the country," Dr. Freedman said. "In an ordinary size city, it's a city block. In New York City, you might split a block. In rural Montana, you might take acres."

Census workers go to those areas and seek out every resident. They compare their data with those obtained in the original census and ask, whom did they find who previously was missed? And whom did they miss who previously was found? From that information, the idea is to use statistics to project the error rates to every one of the seven million blocks (or their acre equivalents) in the country.

But the census workers who go back will make their own errors in counting and in matching up their people with those found before, Dr. Freedman said. The new numbers will be different, but not necessarily better, he said. Instead of making progress, he said, the counts may be just "going sideways."

The nation's suddenly notorious voting problem is similar. After the Florida election, cries went out to improve the accuracy of voting by getting rid of the old punch cards with their fickle chads. Less error-prone machines, like touch-screen versions, are expensive—Riverside County in California just spent nearly \$14 million on 4,250 machines. But you can't accidentally vote twice, and there should be no ambiguity about whom you voted for. Over all, accuracy tends to go up.

But, as with any computer solution, the problem is that not only can the machines introduce errors but the errors can be much harder to detect, Peter Neumann, a computer scientist at SRI International in Menlo Park, Calif., warned.

What if there is a tiny glitch in the software or the hardware? How would you know if 1 out of every 100,000 votes goes to someone other than the intended candidate? What if the misdirected votes were created by programmer sabotage?

"There is no guarantee that your vote goes into the computer the way it looked on the touch screen," Dr. Neumann said. One thing is sure: with touch-screen computers, there is no chance for a recount.

Last week, after jamming supermarkets and lining up at gas stations to fill their tanks in preparation for a monster snowstorm that essentially missed them, New Yorkers were amused, disappointed, and, in some cases, angry. Can't the weather forecasters get it right?

No, said Bob Gall, the lead scientist for the United States Weather Research Program. "The error we're seeing in the forecast of something like the storm on the East Coast is probably close to the limit of technology today," he said. It is impossible, because of measurement errors, to perfectly specify atmospheric conditions at any one time, he said. And once the conditions are plugged into a computer program, any tiny error gets compounded. The bulk of a storm can—did—end up in Connecticut, not Manhattan.

"If you go out six hours, it can be pretty accurate," Dr. Gall said of weather projections. "Two days can be problematic. At 10 days, you can get almost anything."

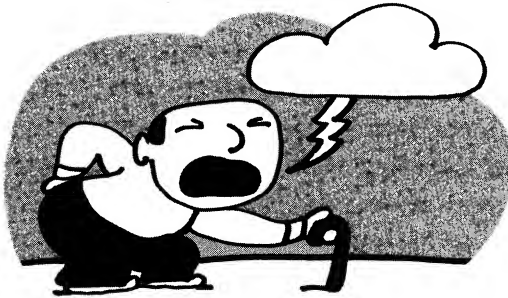
One historian, Edward Tenner, now a visiting researcher at Princeton, who keeps a file on counting problems, says the census and the voting quandaries are typical of what always occurs when people try to change a way of formulating a number. The trick, he said, is either to learn to live with known inaccuracies or to be sure that any new number is really an improvement.

The issue reminds him of the unopened packs of cigarettes bartered in Europe after World War II. "Everyone knew they were probably stale, but as long as no one opened them, you couldn't be sure," he said. "A lot of numbers are like that. As long as you accept them at face value, they work. They are based on a common suspension of inspection." But, he said, the moment that stance is abandoned, "you have a very hard time agreeing again on another standard."

March 11, 2001

Could It Be? Weather Has Nothing to Do with Your Arthritis Pain?

By GINA KOLATA



O.K. Maybe sugar does not make children hyperactive. Maybe getting cold and damp does not predispose people to catch a cold. Maybe there is even no such thing as the “hot hand” in basketball. But surely people with arthritis suffer

more when the weather changes. Surely all those tales of old people who can feel a storm coming in their bones cannot be wrong?

Dr. Amos Tversky, a Stanford University psychologist (and the man who found a decade ago that the “hot hand,” the notion that basketball players on a shooting streak were actually beating the laws of probability, was a myth), begs to differ. He has done a new study and reports that arthritis pain may have nothing to do with barometric pressure or dampness or humidity. Instead, he said, patients’ enduring belief that their arthritis pain is related to the weather is caused by an innate human tendency to find patterns whether they are there or not.

“It’s what I do for a living: debugging human intuition,” Dr. Tversky said. “If you take the broader view and look at people as intuitive scientists, you find that we are very good at pattern generation, we are very good at generating hypotheses. It’s just that we are not very good at all at actually testing hypotheses.” It is easy for humans to guess that an association exists. But testing and, if necessary, rejecting such associations tends to go against all our intuitions, he explained.

The conviction that joint pain ebbs and flows with the weather dates to Hippocrates in 400 B.C., Dr. Tversky said. But the medical literature on arthritis pain and weather is conflicting and confused, the researchers found. Studies that objectively measured inflammation found no associations with weather patterns.

Studies that used subjective measures of pain sometimes found associations and sometimes did not. Some investigators found that pain increased when barometric pressure increased, but others found that pain decreased when barometer readings rose. Some found that pain occurred only when both barometric pressure and humidity changed, but others found no such correlation. Some studies found that weather affected arthritis pain immediately, but others said it took a few days for the effects of weather to show up.

So Dr. Tversky and a colleague, Dr. Donald A. Redelmeier, an internist at the University of Toronto, conducted their own study, which is published in the current issue of *Proceedings of the National Academy of Sciences*. They recruited 18 patients with arthritis and followed them for 15 months, assessing pain as reported by the patients; joint tenderness, as determined by a doctor; and the patients' functional status, the ability to get along in daily life, as measured by a standard test. They also obtained local weather reports on temperature, barometric pressure and humidity.

All but one of the patients were convinced that their arthritis pain varied with the weather and all but two said that it was a powerful effect, occurring within a day of a weather change and that the relevant variables were barometric pressure, temperature or humidity.

But the researchers found no correlation between the patients' symptoms and the weather, no matter what aspect of weather they looked at. They even considered nine different time lags, from two days before to two days after a patient reported pain, but the weather simply was not related to pain, they found.

The best explanation, Dr. Tversky said, is that the human brain is designed to look for patterns, even if, statistically, patterns do not exist. Dr. Tversky said he could understand why people might attribute arthritis pain to the weather. "If your joints ache, you look for a reason," he said. "If it's not rain, it's barometric pressure. If it's not barometric pressure, it's humidity." Dr. Redelmeier said that "the longer you live with arthritis, if anything the greater your degree of confidence" that weather influences your pain.

Dr. Persi Diaconis, a professor of mathematics at Harvard University, said that even as a scientist who studied the laws of probability, he found himself seeing patterns in random data. "We all know how easy it is to do this," he said. In fact, he said, laboratory research has shown that people tend to make up elaborate rules to explain what are actually random events.

One such experiment involved two lights in a room. One would be flipped on and the other flipped off in a randomly generated sequence that forced the light on the left to be turned on 70 percent of the time and the one on the right to be flipped on 30 percent of the time.

Volunteers were paid every time they correctly guessed which light would turn on next. Of course, Dr. Diaconis said, since there was no pattern, the best strategy would be to guess the left light every time; then you would be right 70 percent of the time. Instead, he said, people made up their own elaborate rules, like: after two lefts it is a right except after five times the left light goes on twice in a row. "Dumb creatures like goldfish actually do better than people," Dr. Diaconis said.

Dr. Tversky and Dr. Redelmeier did a small experiment along the same lines. They generated sequences of random numbers and labeled one sequence "arthritis pain" and the other "barometric pressure." They then asked 97 college students if they saw evidence in the data that pain was correlated with barometric pressure. They did, finding patterns where there were none.

When it comes to real arthritis pain, Dr. Tversky and Dr. Redelmeier may have some trouble getting their point across. Dr. Michael Lockshin, a rheumatologist at the National Institutes of Health in Bethesda, Md., said most patients were already convinced of the relationship and often asked their doctors if they should move to a place like Arizona. Many doctors also believe that the relationship with weather is real, he said. In fact, he said, in studies in the 1960s, researchers tried and failed to find evidence that joints became more inflamed when the weather changed. So they decided that barometric pressure changes made patients feel more pain, even if their joints were no more inflamed.

Dr. Frank Arnett, a rheumatologist at the University of Texas at Houston, said that he himself remained convinced that the weather influenced arthritis pain.

"It goes well beyond arthritis," Dr. Arnett said. "Actually, anyone who has any disorder of the musculoskeletal system tends to notice pain when the weather changes. Even someone who had a fracture and it heals complains that they can tell when the weather is going to change. My wife had that and she doesn't imagine things. I would find it hard to disregard a notion we had for centuries."

Dr. Redelmeier said he would not argue with patients who were convinced of the weather's influence on arthritis pain.

"My job as a physician is to listen to patients and get rid of their pain," he said. He finds it can do more harm than good to "confront people about their beliefs and try to force them to change their minds."

Dr. Tversky added that he knew from experience that such arguments often fell on deaf ears. As fascinated as he was to find that the hot hand in basketball was a myth, he discovered that no one wanted to hear it and that most people still believed in the phenomenon.

"I've lost many good friends over it," Dr. Tversky said.

April 3, 1996

Electronics to Aid Weather Figuring

By SIDNEY SHALETT

Plans have been presented to the Weather Bureau, the Navy and the Army for development of a new electronic calculator, reported to have astounding potentialities, which, in time, might have a revolutionary effect in solving the mysteries of long-range weather forecasting.

Official sources confirmed today that a conference was held in Washington yesterday, under the sponsorship of the Weather Bureau, at which representatives of the bureau, the Navy and the Army Air Forces Weather Service heard the proposal outlined by the scientists who developed it.

The official sources cautioned that the development still was strictly "on paper," and that, even if the green light should be given at once (which it has not been), that it would take at least two years to produce a practical working model. However, they are "extremely interested" in the possibilities of the projected device, and point out that, while no pilot model has been produced, it is more than a theory, for the plans are based on principles which actually have been proven in smaller-scale operations.

If the super-calculator could be built and operated successfully, weather experts said, it not only might lift the veil from previously undisclosed mysteries connected with the science of weather forecasting, but might even make it possible to "do something about the weather" through advance application of scientific knowledge concerning countermeasures to unfavorable weather. The benefits to agriculture, shipping, air travel and other activities through advance knowledge of the weather were obvious, they added, and the savings in crops, money and even lives would be incalculable.

Dr. John von Neumann, Hungarian-born mathematician who is associated with the Institute of Advanced Study, Princeton University, and Dr. Vladimir Kosma Zworykin, Russian-born scientist and associate director of the Radio Corporation of American Laboratories at Princeton, developed the plans for the new machine.

RCA and Princeton have been jointly instrumental in promoting the research, which has now reached the stage where the plans could be laid before the government departments which would be vitally interested.

Both Doctors von Neumann and Zworykin were present yesterday at the conference at which their device was explained. No decisions were taken which

would lead to immediate construction of the electronic calculator, but the conferees agreed that there should be further talks at which there should be discussion of whether the government shall finance the project.

Mathematical Approach

Adaptation to mathematical problems relating to weather forecasting is the primary purpose of the projected device, but experts see no reason why the machine, if it materializes, should not be useful in other fields. Naval Ordinance, for instance, is interested in the device.

No cost estimates were presented, but officials agreed that millions of dollars would probably be required to develop and build an "adequate" number of such machines.

The electronic calculator, as conceived by Drs. von Neumann and Zworykin, is a device which would be able to perform the most incredibly complicated and advanced equations in conceivably minute fractions of a second. One scientist who attended the conference said that it was expected to be capable of performing a multiplication in eleven microseconds (eleven millionths of a second), and that it would solve 100,000 different equations in about one minute.

According to Navy meteorologists, the great problem in weather forecasting at present is the lack of any means to work out all the mathematical variables within the time that such knowledge would be useful. In other words, meteorologists say they believe they know in theory what should be done about correlating all the complex factors that would shed light on what the weather would be one month or two months hence, but that they were hopelessly bogged down by inability to solve the mathematical equations quickly enough.

This new machine—if it can be constructed successfully—should be capable of grinding out the answers automatically and speedily. It would provide (a) a greater fund of mathematical information necessary to weather forecasting, and (b) more accurate information, and these two factors combined should make possible longer-range forecasts, that is, accurate forecasts weeks or perhaps even months in advance.

A number of extremely advanced calculating machines have been built. Some are mechanical and some employ electronic principles, but on a limited scale. One of the most widely publicized of the calculators is the so-called "Harvard machine," capable of solving highly complex problems.

None of the existing machines, however, is as pretentious in scope as the von Neumann-Zworykin device. For example, a Navy expert pointed out that one of the most advanced of the existing machines has a "memory" of twelve numbers; that is, it can solve problems that go into twelve stages. The projected calculator would solve problems running into 400 stages.

Weather Bureau, Navy and Army Air Force experts all were represented as interested in the project. A Navy aerologist went on record as saying that "the Navy is definitely interested and considers the proposal promising." Dr. Francis W. Reichelderfer, chief of the Weather Bureau and head of the National Weather Service, said the Weather Bureau was "extremely interested."

The device, Dr. Reichelderfer added, has "some very far-reaching and, we hope, revolutionary possibilities" in the field of long-range weather forecasting. His general attitude was one of "hopefulness and optimism," though he said he wished to caution strongly that realization of the project "is not just around the corner." He felt that the two-year minimum estimate was on the optimistic side.

Machine 12 Feet High in Mind

The device would be roughly about 12 feet high, 18 feet wide and 20 feet long. It would use perhaps as many as 2,000 electronic tubes of various types and its interior would be a maze of wires and controls, separated by air spaces in which workmen could operate. It would require perhaps 10 to 20 persons to operate the machine.

Meteorologists contemplate that with enough of these machines (100 was mentioned as an arbitrary figure) area stations could be set up which would make it possible to forecast the weather all over the world. The United States would be divided into "blocks" penetrating into the stratosphere, and every condition which would have any bearing on the weather would be analyzed.

Plans for the machine even provide for an "alarm" which would give a warning if any error in calculation occurred.

Some Washington officials responsible for investigating the plan feel that such a device, if it can be developed, offers limitless possibilities. They use the word "revolutionary" advisedly, for they feel that the science of forecasting—and perhaps controlling—the weather is on the verge of unprecedented advances.

Mark Twain once observed that every one talks about the weather but no one does anything about it. That no longer is exactly true, as there have been

successful—though small-scale—experiments in combating such conditions as frost and fog. Now scientists ask why it should not be possible to head off such disasters as typhoons, hurricanes and violent rainstorms if there is knowledge sufficiently in advance of where and when they will strike.

Some scientists even wonder whether the new discovery of atomic energy might provide a means of diverting, by its explosive force, a hurricane before it could strike a populated place.

January 11, 1946

Insurance as a Study; Something of the Men Who Figure Business by Algebra

Last week's meeting in this city of the Society of Actuaries developed some interesting facts in relation to life insurance. Actuaries are the mathematicians of insurance companies. They are employed and relied upon to establish formulae upon which the insurance business may be profitably carried on. The study of figures makes up their work, and they apply their mathematical talent to all kinds of tables that interest insurance men.

In a business involving such large amounts of money as that of life insurance, nothing except the most expert talent is employed for this work. There are but thirty-four companies in this country doing regular life insurance business, although the number of assessment companies is legion.

The papers submitted at the meeting last week abounded in algebraic formulae to express business propositions. Some of these formulae were not wholly new, but in nearly every case they received a fresh application to facts and figures which the actuaries understand. Some idea of the responsibility devolving on these officers may be judged from the total of business done by the life insurance companies.

The assets of the companies doing business in this country was \$811,186,000 for the year ending last December. The companies paid out in death claims in 1891 \$60,131,000. They paid for surrendered policies and dividends \$29,814,000. There were insurances outstanding at the end of the year of \$4,133,439,000, insuring 4,176,435 persons. These totals include industrial insurance. The industrial companies insure in sums running from \$25 to \$1,000, but the average of insurances in the large companies is about \$3,500.

There is no country in the world in which the volume of life insurance business is anything like as large as it is in this country. State supervision of this business, which obliges the insurance companies to report annually the amount of insurance carried by them, and their assets and liabilities, provides accurate statistics upon the subject. It is not so easy to get similar statistics for other countries, because elsewhere there is no governmental supervision of this business, and the details furnished in the insurance reports here are not easily obtainable elsewhere. Foreign companies make reports to their stockholders, but, as a rule, are not concerned with letting the general public know what they do.

The 34 companies doing business in this country carry much more insurance in the aggregate than about 100 regular companies in Great Britain and Ireland. The aggregate is enormously in excess of companies in other countries. Canada has 10 companies, Austria 19, Belgium 2, the Netherlands 9, France 21, Germany 52, Italy 2, Russia 5, and Scandinavia 17.

In England, France, and Germany, the Institute of Actuaries is regarded as a very important body. The London Institute has been established since 1848. Its work consists not merely of meetings of actuaries for the comparison of ideas, but it has established a course of study for persons intending to become actuaries.

Out of the London Institute of Actuaries has also grown a club known as the Insurance Musical Society of London. This is said to be quite a flourishing affair, and it is maintained not simply to provide social diversion to its members, but because of the settled conviction among actuaries that mathematics and music as so closely related that a club of this kind is the most natural thing in the world.

May 2, 1892

Leontief's Contribution

By LEONARD SILK

Long before giant electronic computers were available to solve the scores of simultaneous questions that make up an input-output model of the national economy, Wassily Leontief was slaving away to assemble and compute the data that would show precisely how the American economy fits together and works—the input-output method of economic analysis.

By “input” Professor Leontief means the goods and services that each industry buys from others, and “output” means the products that each industry turns out and sells to others.

The entire American economy—or that of any other country or group of countries—thus can be conceived of as a giant, tic-tac-toe grid—a “matrix,” in the language of mathematicians.

All industries are listed down the left side of the grid, one industry per row; and all industries are also listed across the top of the grid, one industry per column.

From One to Another

Every number given in the cells of the grid simultaneously represents an input and an output. From the standpoint of the industry at the left of each row, each number represents a part of its output—what it sells to the industries arrayed at the top of the grid. The sum of those sales represents its total output.

From the standpoint of each industry at the top of every column, each number below represents an input that it uses in making its own products.

The output of, say, the steel industry includes its sale to the auto industry, the construction industry, and so on. And the steel industry itself receives inputs from the construction industry, the chemical industry, the railroad industry (especially trucks), and so on, in order to produce its output.

This is the essentially simple theoretical concept that Professor Leontief struck upon when he was a young student in Leningrad. (The Russians proudly claim title to his first theoretical input-output paper.) He developed the concept into a useful tool for economic analysis, forecasting and planning during his subsequent years at Harvard and his occasional tours of temporary duty in the United States government.

High-Class Math Needed

Although Professor Leontief is the undisputed founding father of input-output analysis, he was not the first economist who dreamed of building a model to show the way goods flowed from one industry to another. That honor goes to an 18th-century French economist François Quesnay, who created a so-called *tableau economique*, designed to prove the “physiocratic” doctrine that agriculture was the source of all wealth—because the farmer fed his product to the landowner and the “class sterile”—the manufacturers.

Quesnay’s *tableau*, which contained theoretical mistakes and poor data, can correctly be restated as a simple three-sector Leontief model, with farmers, landlords and artisans as the producers of outputs and the consumers of each other’s inputs.

All that the world needed to put the Quesnay-Leontief concept to work—as more than 50 countries have done—was some high-class mathematics for solving all those simultaneous equations, the electronic computer to lift the process up from laborious academic fun and games to practical government and business use, and masses of data.

Professor Leontief has been a constant scold in the economics profession for what he regards as its overemphasis on abstract theory and highfalutin model-building and its underemphasis on the gathering of empirical data.

In his presidential address to the American Economic Association three years ago, he denounced his colleagues, for the “palpable inadequacy of the scientific means” by which they were trying to solve problems, especially for under-rating the importance of observation and measurement in the classic Baconian four-term conception of scientific method—observation, measurement, explanation and verification.

Professor Leontief’s industriousness in pressing on with the detailed empirical fleshing out of his essentially simple theoretical idea has borne much fruit, some of it strange and unexpected.

One is the so-called Leontief Paradox—his finding that in the United States capital rather than labor is the relatively scarce factor of production.

Solving Special Problems

Another contribution has been to the development of linear programming—a mathematical technique for solving involved problems of economic operations,

such as how to schedule oil-refinery runs or where to locate auto plants.

He has turned his hand to many other optics, theoretical as well as empirical, including index numbers of prices and quantities, problems of aggregation, economic growth, automation and the nature of knowledge as a unique and inexhaustible good. He has flirted with philosophy, business and politics, and was an adviser to George McGovern in the 1972 campaign.

First and foremost he is an economic scientist. His colleagues have sometimes faulted him for not building complex enough models of the economy that would be more dynamic and sensitive to the effects of changing prices, interest rates and other variables.

However, Professor Leontief—no mean theorist himself—decided that what he was doing was complicated enough already and that he would be happy if he could just get current relations among industries reasonably straight. His modest hope was that those interindustry relations would be technologically stable enough to be used as a tool for analysis and planning.

October 19, 1973

Many Small Events May Add Up to One Mass Extinction

By MALCOLM W. BROWNE

Did the mass extinctions that have punctuated the history of life on this planet have a common cause, or were they just statistical fluctuations nudged to extremes by many unrelated causes?

Since 1980, heated scientific debates have arisen from this and related questions. Many disagreements have centered on the wave of extinctions at the end of the Cretaceous period some 65 million years ago that saw the demise of the dinosaurs, the marine shellfish called ammonites, and many other large groups of animals.

Partisans of various opposing theories have argued that major mass extinctions throughout the 3.5-billion-year history of life on earth have been caused by the impact of large meteors, by volcanic eruptions that covered an area the size of a continent, by protracted ice ages, by changes in sea level, epidemics and many other factors.

But a collaboration of European scientists has raised another possibility: mass extinctions may be caused by complex, interacting conditions that cannot be encompassed by any simple explanation.

The scientists reported in the Aug. 21 edition of the journal *Nature* that their analysis of data culled from the fossil record reveals statistical patterns over time that mathematicians describe as "fractal." In this kind of pattern, the frequency of an event taking place is inversely proportional to its intensity; for example, the statistical expectation is that there will be a certain number of small earthquakes for every large one.

The report suggests that extinctions of all magnitudes, from the smallest to the most devastating, probably had many different causes and that future mass extinctions may be intrinsically unpredictable.

Moreover, the impact of an asteroid or a continental blast of volcanic lava may not be needed to kill off a large proportion of the earth's animals and plants, the authors said; relatively small changes in global conditions may sometimes combine in complex ways to precipitate catastrophic consequences.

There is growing evidence that the mass extinction at the end of the Cretaceous period occurred about the same time that a monster meteor struck

the Yucatán Peninsula. And yet, efforts to link other major extinctions with similar impacts have largely failed.

One of the authors of the *Nature* paper, Dr. Michael J. Benton, a paleontologist at the University of Bristol, England, said in an interview that he believes the Cretaceous extinction was the only one of the "big five" mass extinctions for which there is fairly good evidence that a large meteor impact occurred about the same time. (The other four occurred at the end of the Cambrian period 500 million years ago, at the end of the Devonian period 350 million years ago, at the end of the Permian period 230 million years ago—the most devastating of all—and at the end of the Triassic period 195 million years ago.)

Moreover, there are several meteor craters of about the same size as the Yucatán crater (110 miles in diameter) that do not correspond in time to any known mass extinction, Dr. Benton said.

The European study was headed by Ricard V. Solé, a physicist at the Polytechnic University of Catalonia, Barcelona, with his student, Susanna C. Manrubia, with Dr. Benton and Dr. Per Bak, a physicist at the Niels Bohr Institute in Copenhagen, Denmark.

The European scientists who conducted the new study culled statistics from the fossil record and concluded that extinctions large and small fit a fractal pattern known as "scale-invariant self-similarity." This means, roughly, that a common statistical pattern pervades a certain class of things, regardless of how the size scale varies.

According to ideas pioneered by a French mathematician, Dr. Benoit Mandelbrot, fractal patterns manifest themselves throughout nature. Thus, the jagged pattern of a shoreline seems much the same at all scales, whether viewed in fine detail from an inch above or in gross outline a mile above.

In the European study, the supposed fractal scale is based on increments of time during which extinctions took place. The scientists plotted patterns of extinctions over different time scales, and found that the patterns over large intervals of time seemed similar (although different in scale) to patterns within smaller time scales. They conclude that the erratic responses of the earth's "biosphere" to perturbations—including small ones, like the normal fluctuations in the ratios between competing species "provide the main mechanism for the distribution of extinction events."

This neither supports nor weakens any particular theory on how the dinosaurs or any other group became extinct. Mathematically speaking, Dr. Benton

said, it is equally possible for an extinction to have been the result of the internal dynamics of an ecosystem, or an asteroid impact, or any other influence.

But as scientists try to discern a coherent pattern underlying the mass extinctions, doesn't the new report amount to a frustrating return to the starting line?

"Yes, I think that's right," Dr. Benton said. "I think the mathematics are perfectly concordant with the idea of all kinds of crises contributing to extinctions, with no explanation particularly favored."

Among the critics of this view is Dr. David M. Raup, a statistical paleontologist who retired several years ago from the University of Chicago.

Dr. Raup has argued for more than a decade that most extinctions—minor waves as well as globally catastrophic ones—result from meteor impacts. The quest for subtle biological interactions and for complex mathematical models to explain how they can add up to mass extinctions is futile, he said, because the evidence is that some 60 percent of all extinctions are caused by extraterrestrial matter: comets, asteroids and other small objects.

Regarding Dr. Bak's notion that extinctions occur in fractal patterns independently of specific causes, Dr. Raup said in an interview: "It's intuitively wonderful. A very cuddly idea. But I don't buy it."

Statistical explanations of this kind remind him, he said, of the ideas of Dr. René Thom, a French mathematician whose "Catastrophe Theory" was popularized in the 1970s as a mathematical model for explaining the abrupt onset of wars, traffic jams, stock crashes, chemical reactions and much more.

Catastrophe theory was based on analyses of the topology, or surface structure, of abstract mathematical shapes endowed with "cusps." These cusps, like the tips of upward pointing needles, were places where an object could be sent flying with equal probability in several possible directions, with the slightest push.

"Physicists' theories that attempt to explain everything can end up explaining nothing," he said.

September 2, 1997

Metric Mania

By JOHN ALLEN PAULOS

In the realm of public policy, we live in an age of numbers. To hold teachers accountable, we examine their students' test scores. To improve medical care, we quantify the effectiveness of different treatments. There is much to be said for such efforts, which are often backed by cutting-edge reformers. But do we hold an outsize belief in our ability to gauge complex phenomena, measure outcomes and come up with compelling numerical evidence? A well-known quotation usually attributed to Einstein is "Not everything that can be counted counts, and not everything that counts can be counted." I'd amend it to a less eloquent, more prosaic statement: Unless we know how things are counted, we don't know if it's wise to count on the numbers.

The problem isn't with statistical tests themselves but with what we do before and after we run them. First, we count if we can, but counting depends a great deal on previous assumptions about categorization. Consider, for example, the number of homeless people in Philadelphia, or the number of battered women in Atlanta, or the number of suicides in Denver. Is someone homeless if he's unemployed and living with his brother's family temporarily? Do we require that a woman self-identify as battered to count her as such? If a person starts drinking day in and day out after a cancer diagnosis and dies from acute cirrhosis, did he kill himself? The answers to such questions significantly affect the count.

Second, after we've gathered some numbers relating to a phenomenon, we must reasonably aggregate them into some sort of recommendation or ranking. This is not easy. By appropriate choices of criteria, measurement protocols and weights, almost any desired outcome can be reached. Consider those ubiquitous articles with titles like "The 10 Friendliest Colleges" or "The 20 Most Lovable Neighborhoods." Such articles would be more than fluff if they answered critical questions. Are there good reasons the authors picked the criteria they did? Why did they weigh the criteria in the way they did? If changes in the criteria were made, would the rankings of the friendliest colleges or most lovable neighborhoods be vastly different?

Since the answer to the last question is usually yes, the problem of reasonable aggregation is no idle matter. Recently released e-mail from employees at the credit-rating agency Standard & Poor's indicated a wish to "discuss adjusting

criteria" for rating securities and "massage the subprime and alt-A numbers to preserve market share." The criteria adjustments were analogous to the adjustments that would put an area of abandoned buildings onto the list of the most lovable neighborhoods.

These two basic procedures—counting and aggregating—have important implications for public policy. Consider the plan to evaluate the progress of New York City public schools inaugurated by the city a few years ago. While several criteria were used, much of a school's grade was determined by whether students' performance on standardized state tests showed annual improvement. This approach risked putting too much weight on essentially random fluctuations and induced schools to focus primarily on the topics on the tests. It also meant that the better schools could receive mediocre grades because they were already performing well and had little room for improvement. Conversely, poor schools could receive high grades by improving just a bit.

Medical researchers face similar problems when it comes to measuring effectiveness. Consider the temptation to use the five-year survival rate as the primary measure of a treatment for a particular disease. This seems quite reasonable, and yet it's possible for the five-year survival rate for a disease in one region to be 100 percent and in a second region to be 0 percent, even if the latter region has an equally effective and cheaper approach.

This is an extreme and hypothetical situation, but it has real-world analogues. Suppose that whenever people contract the disease, they always get it in their mid-60s and live to the age of 75. In the first region, an early screening program detects such people in their 60s. Because these people live to age 75, the five-year survival rate is 100 percent. People in the second region are not screened and thus do not receive their diagnoses until symptoms develop in their early 70s, but they, too, die at 75, so their five-year survival rate is 0 percent. The *laissez-faire* approach thus yields the same results as the universal screening program, yet if five-year survival were the criterion for effectiveness, universal screening would be deemed the best practice.

Because so many criteria can be used to assess effectiveness—median or mean survival times, side effects, quality of life and the like—there is a case to be made against mandating that doctors follow what seems at any given time to be the best practice. Perhaps, as some have suggested, we should merely nudge them with gentle incentives. A comparable tentativeness may be appropriate when devising criteria for effective schools.

Arrow's Theorem, a famous result in mathematical economics, essentially states that no voting system satisfying certain minimal conditions can be guaranteed to always yield a fair or reasonable aggregation of the voters' rankings of several candidates. A squishier analogue for the field of social measurement would say something like this: No method of measuring a societal phenomenon satisfying certain minimal conditions exists that can't be second-guessed, deconstructed, cheated, rejected or replaced. This doesn't mean we shouldn't be counting—but it does mean we should do so with as much care and wisdom as we can muster.

May 13, 2010

In Shuffling Cards, 7 Is a Winning Number

By GINA KOLATA

It takes just seven ordinary, imperfect shuffles to mix a deck of cards thoroughly, researchers have found. Fewer are not enough and more do not significantly improve the mixing.

The mathematical proof, discovered after studies of results from elaborate computer calculations and careful observation of card games, confirms the intuition of many gamblers, bridge enthusiasts and casual players that most shuffling is inadequate.

The finding has implications for everyone who plays cards and everyone, from casino operators to magicians, who has a stake in knowing whether a shuffle is random.

The mathematical problem was complicated because of the immense number of possible ways the cards in a deck can be arranged; any of 52 could be first in the deck, any of 51 could be second, 50 could be third and so on. Multiplied out, the number of possible permutations, 52 factorial, or 52; 51; 50, etc. is 10^{63} or 10 with 62 zeros after it.

No one expected that the shuffling problem would have a simple answer, said Dr. Dave Bayer, a mathematician and computer scientist at Columbia who is a co-author of the recent discovery. Other problems in statistics, like analyzing speech patterns to identify speakers, might be amenable to similar approaches, he said.

The new result "definitely solves the problem," said Dr. David Aldous, a statistician at the University of California at Berkeley. "All their calculations are right. It's a fascinating result." Dr. Persi Diaconis, a mathematician and statistician at Harvard University who is the other author of the discovery, said the methods used are already helping mathematicians analyze problems in abstract mathematics that have nothing to do with shuffling or with any known real-world phenomena.

Dr. Diaconis, who is also a magician, has invented numerous card tricks and has been carefully watching casino dealers and casual card players shuffle for the past 20 years. The usual shuffling produces a card order that "is far from random," Dr. Diaconis said. "Most people shuffle cards three or four times. Five times is considered excessive."

The realization that most shuffled decks are not actually random allows gamblers to improve their odds of winning. "There are people who go to casinos and make money on this," Dr. Diaconis said. "I know people who are out there doing that now."

How Casinos Do It

In Las Vegas, cards are shuffled from four to seven times, at the discretion of the casino owners, said Richard Ingram, a Las Vegas enforcement agent for the state gambling control board. Dr. Diaconis said he almost never sees a dealer shuffle seven times. He said his research also shows that when dealers shuffle several decks at once, they need to shuffle more. Two decks should be shuffled nine times, he said, and six decks should be shuffled twelve times, which is unheard of in the casinos.

At Trump Plaza in Atlantic City, blackjack dealers shuffle eight decks twice at the beginning of each game, said Howard Dreitzer, who is senior vice president of casino operations. "We've tested these shuffles and feel that they are random," he said, adding that "no one has ever complained."

Bridge players usually shuffle about four times, except in some tournaments when a computer randomly mixes the cards, said Edgar Kaplan, who is editor and publisher of *Bridge World* magazine. Asked whether he expected bridge players to change their shuffling habits, Mr. Kaplan replied, "There will be a few who will be affected and will doggedly shuffle seven times to the irritation of everyone else." As for himself, Mr. Kaplan said, "I probably will move up from four to five" shuffles, a decision which, the research shows, will not appreciably improve the randomness of the shuffled cards.

Dr. Diaconis has found that many bridge players take advantage of the non-randomness of seemingly shuffled cards. He said a bridge club in New York State once consulted him, as a magician, to find out whether several players were cheating. After watching play "and doing a little thinking in between," Dr. Diaconis knew what was going on. These players had figured out that the cards were not being randomly shuffled, and that they could predict the distributions of cards by knowing what the deck looked like at the end of the previous hand.

A Punishment of Sorts

The players "admitted to it readily," Dr. Diaconis said. "But they didn't think they were doing anything wrong. After all, they were just thinking." The club asked those players not to play together for a year.

When computers were introduced into tournament bridge about 18 years ago, some players were puzzled and others outraged by the random hands the computer dealt and complained that the computers were not working right.

At about the same time, a bridge encyclopedia was published. The encyclopedia "used a computer to figure out odds," Dr. Diaconis said. "For example, given that between my opponents there are seven hearts, what's the chances that one has four hearts and the other has three? Some of these odds were at variance with expert play. The experts had intuited—correctly—the actual ways the cards were shuffled. People thought the encyclopedia was wrong."

By saying that the deck is completely mixed after seven shuffles, Dr. Diaconis and Dr. Bayer mean that every arrangement of the 52 cards is equally likely or that any card is as likely to be in one place as in another.

The cards do get more and more randomly mixed if a person keeps on shuffling more than seven times, but seven shuffles is a transition point, the first time that randomness is close. Additional shuffles do not appreciably alter things.

Grist for Magicians

Magicians have long taken advantage of the non-randomness of most card shuffling, Dr. Diaconis said. In fact, he said, Charles T. Jordan, a magician, chicken farmer and professional contest entrant from Petaluma, Calif., made a fair amount of money around the turn of the century by selling a card trick exploiting the fact Dr. Diaconis said he first began to think about the shuffling problem 20 years ago after a visit to A.T.&T. Bell Laboratories in Murray Hill, N.J. Mathematicians there told him about the problem but said they had given up trying to solve it in 1955 because there were so many ways to arrange a deck.

Dr. Diaconis began working with Dr. Jim Reeds at Bell Laboratories and showed that a deck is perfectly mixed if it is shuffled between 5 and 20 times.

Next, Dr. Diaconis worked with Dr. Aldous and showed that it takes 5 to 12 shuffles to perfectly mix a deck. But, said Dr. Diaconis, "nobody in practice shuffles 12 times," adding, "We needed some new ideas."

In the meantime, he also worked on "perfect shuffles," those that exactly interlace the cards. Almost no one except a magician can do perfect shuffles every time. But Dr. Diaconis showed several years ago that if a person actually does perfect shuffles, the cards would never be thoroughly mixed. He derived a mathematical proof showing that if a deck is perfectly shuffled eight times, the cards will be in the same order as they were before the shuffling.

To find out how many ordinary shuffles were necessary to mix a deck, Dr. Diaconis and Dr. Bayer watched players shuffle. He also watched Las Vegas dealers to see how perfectly they would interlace the cards they shuffled.

Observations during Poker

Dr. Bayer said he seized every opportunity to get data. "I asked everyone in my poker game, once they dropped out of a hand, to shuffle for me," he said.

Then the researchers did extensive simulations of shuffling on a computer. To get the proof, the researchers looked at a lot of shuffles, guessed that the answer is seven, and finally proved it by finding an abstract way to describe what happens when cards are shuffled.

"When you take an honest description of something realistic and try to write it out in mathematics, usually it's a mess," Dr. Diaconis said. "We were lucky that the formula fit the real problem. That is just miraculous, somehow."

January 9, 1990

Can Game Theory Predict When Iran Will Get the Bomb?

By CLIVE THOMPSON

Many people wonder, but Bruce Bueno de Mesquita claims to have the answer.

Bueno de Mesquita is one of the world's most prominent applied game theorists. A professor at New York University and a senior fellow at the Hoover Institution at Stanford, he is well known academically for his work on "political survival," or how leaders build coalitions to stay in power. But among national-security types and corporate decision makers, he is even better known for his prognostications. For 29 years, Bueno de Mesquita has been developing and honing a computer model that predicts the outcome of any situation in which parties can be described as trying to persuade or coerce one another. Since the early 1980s, C.I.A. officials have hired him to perform more than a thousand predictions; a study by the C.I.A., now declassified, found that Bueno de Mesquita's predictions "hit the bull's-eye" twice as often as its own analysts did.

Last year, Bueno de Mesquita decided to forecast whether Iran would build a nuclear bomb. With the help of his undergraduate class at N.Y.U., he researched the primary power brokers inside and outside the country—anyone with a stake in Iran's nuclear future. Once he had the information he needed, he fed it into his computer model and had an answer in a few minutes.

In June, I visited Bueno de Mesquita at his San Francisco home to see the results. A tall man with a slab of gray hair, Bueno de Mesquita, who is 62, welcomed me with painstakingly prepared cups of espresso. Then he pulled out his beat-up I.B.M. laptop—so old that the lettering on the A, S, D and E keys was worn off—and showed me a spreadsheet that summarized Iran's future.

The spreadsheet included almost 90 players. Some were people, like the Iranian president, Mahmoud Ahmadinejad, and Supreme Leader Ali Khamenei; others were groups, like the U.N. Security Council and Iran's "religious radicals." Next to each player, a number represented one variable in Bueno de Mesquita's model: the extent to which a player wanted Iran to have the ability to make nuclear weapons. The scale went from 0 to 200, with 0 being "no nuclear capacity at all" and 200 representing a test of a nuclear missile.

At the beginning of the simulation, the positions were what you would expect. The United States and Israel and most of Europe wanted Iran to have virtually no nuclear capacity, so their preferred outcomes were close to zero. In contrast, the Iranian hard-liners were aggressive. "This is not only 'Build a bomb,'" Bueno de Mesquita said, characterizing their position. "It's probably: 'We should test a bomb.'"

But as the computer model ran forward in time, through 2009 and into 2010, positions shifted. American and Israeli national-security players grudgingly accepted that they could tolerate Iran having some civilian nuclear-energy capacity. Ahmadinejad, Khamenei and the religious radicals wavered; then, as the model reached our present day, their power—another variable in Bueno de Mesquita's model—sagged significantly.

Amid the thousands of rows on the spreadsheet, there's one called Forecast. It consists of a single number that represents the most likely consensus of all the players. It begins at 160—bomb-making territory—but by next year settles at 118, where it doesn't move much. "That's the outcome," Bueno de Mesquita said confidently, tapping the screen.

What does 118 mean? It means that Iran won't make a nuclear bomb. By early 2010, according to the forecast, Iran will be at the brink of developing one, but then it will stop and go no further. If this computer model is right, all the dire portents we've seen in recent months—the brutal crackdown on protesters, the dubious confessions, Khamenei's accusations of American subterfuge—are masking a tectonic shift. The moderates are winning, even if we cannot see that yet.

Could this possibly be what will happen? Certainly Bueno de Mesquita has his critics, who argue that the proprietary software he uses can't be trusted and may cast doubt on the larger enterprise of making predictions. But he has published a large number of startlingly precise predictions that turned out to be accurate, many of them in peer-reviewed academic journals. For example, five years before Ayatollah Khomeini died in 1989, Bueno de Mesquita predicted in the journal *PS* that Khomeini would be succeeded by Ali Khamenei (which he was), who himself would be succeeded by a then-less-well-known cleric named Akbar Hashemi Rafsanjani (which he may well be). Last year, he forecast when President Pervez Musharraf of Pakistan would be forced out of office and was accurate to within a month. In *The Predictioneer's Game*, a book coming out next month that was written for a popular audience, Bueno de Mesquita offers dozens more stories of his forecasts. And as for Iran's bomb?

In a year, he said with a wide grin, we'll know if he's right.

"I'm not an Iran expert," Bueno de Mesquita told me cheerfully as we walked down his tree-lined street on our way to grab some Burmese food. Indeed, his career has been built on a peculiar concept: If you want to predict political events, wisdom and expertise, deep knowledge of a country's culture and history, aren't enough. To forecast the future, you need to be an expert not in statecraft but in the way individual people make decisions. You need "rational actor" game theory.

Bueno de Mesquita began studying political science in the 1960s. While working on his dissertation at the University of Michigan on parliamentary politics in India, a professor assigned him William H. Riker's book *The Theory of Political Coalitions*, one of the first works to apply game theory to politics. Game theory is a branch of mathematics that studies the way people will behave in strategic situations—that is to say, when they're making decisions based on how they think other people will make decisions. Generally, game theory assumes that people are always rational and selfish; they're always angling to get what's best for them, which means their behavior can often be predicted. One famous application of rational-choice theory that particularly intrigued Bueno de Mesquita was Duncan Black's analysis of "committee voting," which argues that if two rival candidates are trying to get elected on a single issue—say, taxes—they'll inevitably shift their positions toward the median voter.

Bueno de Mesquita was enthralled by the idea of rendering the messy business of politics and history into precise, logical equations. He began his signature academic work on "the selectorate," or the group of actors who run a country. In Bueno de Mesquita's worldview, there is no such thing as a "national interest" (or "state"). There are just leaders trying desperately to stay in power by building coalitions within their selectorate—buying off cronies in the case of a dictatorship, for example, or producing enough good works to keep hoi polloi happy in a democracy.

When Bueno de Mesquita spotted a logical error in one of Riker's books, he wrote the author a letter; Riker offered Bueno de Mesquita a job in 1972 at the University of Rochester, where a new generation of political scientists was starting to apply formal mathematical models to political analysis.

That's where Bueno de Mesquita began programming his computer model. It is based loosely on Black's voter theory, and it works like this: To predict how leaders will behave in a conflict, Bueno de Mesquita starts with a specific prediction he wants to make, then interviews four or five experts who know the

situation well. He identifies the stakeholders who will exert pressure on the outcome (typically 20 or 30 players) and gets the experts to assign values to the stakeholders in four categories: What outcome do the players want? How hard will they work to get it? How much clout can they exert on others? How firm is their resolve? Each value is expressed as a number on its own arbitrary scale, like 0 to 200. (Sometimes Bueno de Mesquita skips the experts, simply reads newspaper and journal articles and generates his own list of players and numbers.) For example, in the case of Iran's bomb, Bueno de Mesquita set Ahmadinejad's preferred outcome at 180 and, on a scale of 0 to 100, his desire to get it at 90, his power at 5 and his resolve at 90.

Then the math begins, some of which is surprisingly simple. If you merely sort the players according to how badly they want a bomb and how much support they have among others, you will end up with a reasonably good prediction. But the other variables enable the computer model to perform much more complicated assessments. In essence, it looks for possible groupings of players who would be willing to shift their positions toward one another if they thought that doing so would be to their advantage. The model begins by working out the average position of all the players—the "middle ground" that exerts a gravitational force on the whole negotiation. Then it compares each player with every other player, estimating whether one will be able to persuade or coerce the others to move toward its position, based on the power, resolve and positioning of everyone else. (Power isn't everything. If the most powerful player is on the fringe of an issue, and a cluster of less-powerful players are closer to the middle, they might exert greater influence.) After estimating how much or how little each player might budge, the software recalculates the middle ground, which shifts as the players move. A "round" is over; the software repeats the process, round after round. The game ends when players no longer move very much from round to round—this indicates they have compromised as much as they ever will. At that point, assuming no player with veto power had refused to compromise, the final average middle-ground position of all the players is the result—the official prediction of how the issue will resolve itself. (Bueno de Mesquita does not express his forecasts in probabilistic terms; he says an event will transpire or it won't.)

The computer model, in short, predicts coalitions. And computers are much better at doing this than humans, because with more than a few players the number of possible coalitions quickly multiplies. With 40 players, the typical size of one of Bueno de Mesquita's forecasts, there are 1,560 possible pairs to consider just for

starters. This is why, he says, his model often produces surprising results. It's not that it is smarter than humans. But it methodically works through not only the obvious coalitions we know about and expect but also the invisible ones that we don't.

For Bueno de Mesquita, the first prominent use of the model came in 1979, when the State Department was canvassing academics with expertise on India, including Bueno de Mesquita, to see how some parliamentary maneuverings would unfold. Bueno de Mesquita decided to use his first version of the software (which was, as he puts it, "barely working") and his own knowledge of India to determine the power players and each of their numbers. Then the university's mainframe computer worked on the data all night.

In the morning, Bueno de Mesquita said, he was astonished: the predicted victor was a seemingly minor figure, someone discounted by the experts. Bueno de Mesquita shared their opinion, he told me, but he accepted the computer's verdict anyway. "So I called the person back at the State Department, and told him what I had concluded," Bueno de Mesquita went on. "And there was a long, quiet period and some laughing. He said: 'How did you arrive at that? Nobody's saying that.' So I told him I had a little computer model. He just guffawed. He said, 'I wouldn't repeat that if I were you.'"

Three months later, according to Bueno de Mesquita, his prediction turned out to be right.

The son of Jewish immigrants who arrived from Brussels during World War II, Bueno de Mesquita grew up in Manhattan, where his father ran a small publishing company and his mother managed a women's clothing shop. He went to Queens College when he was 16—"way too young," he says—and read history and literature voraciously. (Bueno de Mesquita spent years researching and writing a short novel that defends Ebenezer Scrooge as a kindhearted man.) "He is one the most remarkably intelligent human beings I've met in my life, and Bruce does not hesitate to tell you that," Kevin Gaynor, an environmental lawyer who has twice hired Bueno de Mesquita to advise his corporate clients on "extremely sensitive" government negotiations, told me half-jokingly. "He's not self-effacing. But he's not self-effacing in a charming way." Bueno de Mesquita's voluminous academic work—he has published 16 books and more than 100 papers—is credited with helping to move game theory and mathematical modeling into the mainstream of political science; according to one count, by 1999 fully 40 percent of papers in the *American Political Science Review* used modeling. (The figure was so high it prompted deep consternation among non-game-theory political

scientists.) While few perform the consulting work he does, other game theorists have produced models very similar to Bueno de Mesquita's, and he actively promotes his technique, including training N.Y.U. undergraduates to do similar predictions. He spends half the year at N.Y.U., where he recently finished a four-year stint as the chairman of the political science department, and half the year at the Hoover Institution at Stanford. Under the terms of his academic contracts, he is permitted to spend one day per week during the academic year doing outside consulting.

It is this consulting, more than his academic work, that has made Bueno de Mesquita both well off and controversial. He began offering predictions to the private sector in 1982, when A.F.K. Organski, a former professor of his, suggested they go into business using Bueno de Mesquita's model. Business negotiations, they reasoned, were like international relations in that they involved players trying to wheedle and coerce one another. Soon Bueno de Mesquita and Organski (who died in 1998) acquired clients ranging from Arthur Andersen to Union Carbide, which tapped them for advice on placating the Indian government after the Bhopal chemical spill. Today Bueno de Mesquita's firm essentially consists of himself and Harry Roundell, a former banker at J. P. Morgan who met Bueno de Mesquita when Roundell hired him in 1995 to help the bank figure out how to push for new, favorable regulations in the U.S. They charge \$50,000 and up to do a prediction and offer negotiating tips, and they take on 18 to 20 of these assignments a year. Beyond saying it was "a reasonable amount of money," Bueno de Mesquita would not describe his income from the company.

To produce a corporate prediction, Roundell and Bueno de Mesquita determine the numerical values of the players in a negotiation by interviewing a firm's executives. This can take anywhere from a few hours on the phone to two days of face-to-face conversations. Both men conduct the interviews, and Bueno de Mesquita enters the information into a spreadsheet.

The real value of Bueno de Mesquita's work, several clients told me, is not only in his predicting how a corporate event might unfold. It is also in figuring out how to influence that event. Because Bueno de Mesquita's model forecasts the future by calculating the impact every player has on every other player, round by round, Bueno de Mesquita can go back and see when some players suddenly become more flexible midway through a negotiation. He can thus perform "what if" experiments: What if that person could be persuaded to change his mind? He'll enter new values into the model, manually changing that player's position, then run it again to see if this change recasts the future to his client's advantage. If

it does, Bueno de Mesquita now has a piece of advice: focus on that player in real life, and try to influence him. If there are dozens of players and dozens of rounds, the number of possible "what if" scenarios becomes enormous: it can take Bueno de Mesquita days of peering at his spreadsheets to identify useful pressure points.

One of Bueno de Mesquita's most prominent public consultations occurred in 1999, when Richard Laphorne, then the vice chairman of British Aerospace, asked him to help engineer a \$10 billion acquisition. The British government wanted British Aerospace to form a pan-European firm by merging with the German firm DASA and the French giant Aérospatiale; British Aerospace, however, was more interested in trying to buy the British electronics giant Marconi Electronic Systems. To persuade the British government to approve the Marconi deal, Laphorne asked Bueno de Mesquita to predict the viability of mergers between the German and French firms. The model forecast that the three firms would never be able to agree on terms, and that the Marconi deal was the better option; when Bueno de Mesquita showed his analysis to the government heads, they agreed to permit the Marconi acquisition. "There's nothing shimmy shammy or flip-flop about it," Laphorne says of the logical nature of Bueno de Mesquita's prediction. "It's very clear where the information came from. It has intellectual rigor." Laphorne is now chairman of the U.K. telecommunications company Cable and Wireless; he has used Bueno de Mesquita for seven predictions since, though he would not disclose the subjects.

It is difficult to verify how accurately Bueno de Mesquita's model performs in corporate settings because most firms are loath to discuss his work for them. For most of the cases we discussed, Bueno de Mesquita would disclose details of the negotiation but wouldn't name the firms in question. In other cases, clients would talk to me and praise Bueno de Mesquita's work for them, but they would not disclose verifiable details of specific negotiations. There were a few exceptions: Robert F. Kelley, a retired former partner of Arthur Andersen, described using Bueno de Mesquita for "60 or 70" cases, ranging from internal firing decisions to figuring out how to persuade the U.S. to support China's entry into the World Trade Organization. (Bueno de Mesquita also offered to use his software to predict which of Arthur Andersen's clients—including, at the time, Enron—were likely to engage in financial fraud. But the firm's lawyers, Bueno de Mesquita says, didn't want to use the tool for fear it would put them in awkward legal positions. "Had I been able to convince the firm" to use the model, Kelley says, "I think that Andersen would be alive today.")

Bueno de Mesquita's most regular client by far has been the C.I.A. He says he has performed more than 1,200 predictions for the agency, tackling questions like "How fully will France participate in the Strategic Defense Initiative?" and "What policy will Beijing adopt toward Taiwan's role in the Asian Development Bank?" In 1987, Stanley Feder, a research political scientist for the C.I.A., published a report analyzing forecasts that Bueno de Mesquita's firm did of political events in 27 countries; he found that the success rate of its predictions was the same as that of the C.I.A.'s own analysts, only more precise. (He "got the bull's-eye twice as often," Feder wrote in his report, which was declassified in 1993. No other reports have been declassified since.) Feder noted, for example, that Bueno de Mesquita's model predicted in a forecast done of Italy's budget one year a specific figure that turned out to be off by only 1 percent; the C.I.A. method would predict just a deficit.

Those who have watched Bueno de Mesquita in action call him an extremely astute observer of people. He needs to be: when conducting his fact-gathering interviews, he must detect when the experts know what they're talking about and when they don't. The computer's advantage over humans is its ability to spy unseen coalitions, but this works only when the relative positions of each player are described accurately in the first place. "Garbage in, garbage out," Bueno de Mesquita notes. Bueno de Mesquita begins each interview by sitting quietly—"in a slightly closed-up manner," as Lapthorne told me—but as soon as an interviewee expresses doubt or contradicts himself, Bueno de Mesquita instantly asks for clarification.

"His ability to pick up on body language, to pick up on vocal intonation, to remember what people said and challenge them in nonthreatening ways—he's a master at it," says Rose McDermott, a political science professor at Brown who has watched Bueno de Mesquita conduct interviews. She says she thinks his emotional intelligence, along with his ability to listen, is his true gift, not his mathematical smarts. "The thing is, he doesn't think that's his gift," McDermott says. "He thinks it's the model. I think the model is, I'm sure, brilliant. But lots of other people are good at math. His gift is in interviewing. I've said that flat out to him, and he's said, 'Well, anyone can do interviews.' But they can't."

You might expect Bueno de Mesquita to be the toast of both Washington and Wall Street, constantly in demand for prognostications. Yet he and Roundell have found that it is not so easy to attract clients. This is partly because most of their clients—especially the C.I.A.—swear them to secrecy. (And perhaps also

because, as Roundell says, "Bruce and I are . . . terrible salespeople.") But they have also faced a barrier that's almost existential, a skepticism that computer models can truly predict the outcome of negotiations. The C.I.A., for example, built its own replica of Bueno de Mesquita's original forecast model, but as Feder noted in his report, "the vast majority of analysts" didn't use it because it seemed too rigid. They thought of analysis as reading and pondering until they had an aha! moment—not feeding data points into a computer model and waiting to see what comes up.

When we spoke, Bueno de Mesquita often seemed irritated by resistance to his work. For all his gifts of intuition, he has a Spocklike disdain for gut instinct. When he occasionally hires colleagues to help him with a complex bit of corporate work, he sternly warns them that they must refrain from expressing any personal opinions and describe only what they see in the spreadsheets. Bueno de Mesquita habitually and hissingly disparages traditional political analysis. He is savvy enough to know that nobody likes a scold, yet he can't help himself; he sheepishly admits to becoming "confrontational" when people think mathematical reasoning can't be used. At the C.I.A., Feder told me, "there were some people who found him arrogant, which was maybe a reasonable reaction."

Donald Green, a political scientist at Yale, questions whether Bueno de Mesquita is serving the discipline well. "When I see clips of Bruce at the TED conference," he says, referring to the annual conference promoting ideas in technology, entertainment and design, "I watch the video and I think, wow, this is so far from the typical way in which political scientists of any stripe behave." Some political scientists are openly dubious about the accuracy of Bueno de Mesquita's model. Stephen Walt, a Harvard professor of international affairs, says that Bueno de Mesquita's nonprediction work—like his theory of the "political survival" of heads of state—make him a "respected scholar, deservedly so." It's the predictions that Walt doesn't trust, because Bueno de Mesquita does not publish the actual computer code of his model. (Bueno de Mesquita cannot do so because his former firm owns the actual code, but he counters that he has outlined the math behind his model in enough academic papers and books for anyone to replicate something close to his work.) While Bueno de Mesquita has published many predictions in academic journals, the vast majority of his forecasts have been done in secret for corporate or government clients, where no independent academics can verify them. "We have no idea if he's right 9 times out of 10, or 9 times out of a hundred, or 9 times out of a thousand," Walt says. Walt also isn't impressed by

Stanley Feder's C.I.A. study showing Bueno de Mesquita's 90 percent hit rate. "It's one midlevel C.I.A. bureaucrat saying, 'This was a useful tool,'" Walt says. "It's not like he's got Brent Scowcroft saying, 'Back in the Bush administration, we didn't make a decision without consulting Bueno de Mesquita.'" Other academics point out that rational-actor theory has come under increasing criticism in recent years, as more evidence accumulates that people make many decisions irrationally.

And it's true that there have been cases when Bueno de Mesquita's model has gone awry. In his 1996 book, *Red Flag over Hong Kong*, he predicted that the press in Hong Kong "will become largely a tool of the state"—a highly debatable claim today. (In 2006, Reporters Without Borders noted concerns about self-censorship but said that "journalists remain free in Hong Kong.") In early 1993, a corporate client asked him to forecast whether the Clinton administration's health care plan would pass, and he said it would.

What's more, with corporate clients in particular, there's always the potential problem of reflexivity, of the prediction itself influencing events and making it hard to evaluate the prediction's value. Suppose a firm is told a merger will fail, for example, and abandons its merger efforts. Was the prediction accurate or a self-fulfilling prophecy?

Spending time with Bueno de Mesquita is alternately alarming and reassuring, because he has such confidence in his own predictions about our global fate. Like many, he believes the future of Pakistan is "incredibly distressing" right now, but he has reached this conclusion in his own way: when he and his students modeled its future last year, the power of Al Qaeda and the Taliban in that region grew quickly throughout 2009, far outstripping that of the government and military. Global warming is another area where politics are doomed to fail. World governments are set to meet this December in Copenhagen to commit to firm CO₂-reduction levels—but when Bueno de Mesquita modeled the future of these targets, most countries renege on them. No democratic government will seriously limit CO₂ if it will hurt its citizens economically.

"When people are asked to make personal sacrifices for the greater good in the longer term, they seem to find 1,001 reasons why their particular behavior is so virtuous that this one particular deviation is really O.K.," Bueno de Mesquita told me recently as we talked in his home office. "I have to drive an S.U.V. because I want to protect my little children from a car accident!"

Yet Bueno de Mesquita remains cheerful, almost unnervingly so. Years of peering at his model have shown him that conflicts almost always have hidden

solutions—places where the computer illuminates the sort of leverage that could be employed to create a sudden, useful countercoalition. For example, with Pakistan, his model showed that if the U.S. merely doubled its annual aid from \$700 million to \$1.5 billion, America's influence in the country would significantly jump, while the militants' would drop drastically. Why? Because with that sort of financial flow, corrupt rural officials would suddenly profit more from helping the U.S. than from helping the Taliban.

In the short term, though, Bueno de Mesquita's reputation will be colored by Iran. The last time we met, it was two weeks after the Iranian election, and the opposition protests had been quashed. The hard-liners, I noted, seemed to be winning—did this mean that the prediction was wrong? "The street movement is running out of steam," Bueno de Mesquita agreed. "Shooting people does act as an effective deterrent." But he still maintained that his model was likely to prevail, and that domestic coalitions we might not detect from abroad are gathering to overwhelm the religious conservatives.

He spent that morning looking over his Iranian data, and he generated a new chart predicting how the dissidents' power would grow over the next few months. In terms of power, one category—students—would surpass Ahmadinejad during the summer, and by September or October their clout would rival that of Khamenei, the supreme leader. "And that's huge!" Bueno de Mesquita said excitedly. "If that's right, it's huge!" He said he believed that Iran's domestic politics would remain quiet over the summer, then he thought they'd "really perk up again" by the fall.

Bueno de Mesquita also approved of Obama's hands-off approach. Bueno de Mesquita ran an experimental version of his Iranian model without the U.S. in it as a player at all, and the coalitions that oppose Ahmadinejad and the bomb emerge a few months more quickly. In other words, American meddling is indeed counterproductive; the less America tries to influence Iran, the more quickly Iran will abandon nuclear weapons, if the logic of the computer is correct.

It's a fascinating analysis, but, I wonder, has he given it to anyone in the State Department? He laughed. "I'm working on access."

August 12, 2009

In Modeling Risk, the Human Factor Was Left Out

By STEVE LOHR

Today's economic turmoil, it seems, is an implicit indictment of the arcane field of financial engineering—a blend of mathematics, statistics and computing. Its practitioners devised not only the exotic, mortgage-backed securities that proved so troublesome, but also the mathematical models of risk that suggested these securities were safe.

What happened?

The models, according to finance experts and economists, did fail to keep pace with the explosive growth in complex securities, the resulting intricate web of risk and the dimensions of the danger.

But the larger failure, they say, was human—in how the risk models were applied, understood and managed. Some respected quantitative finance analysts, or quants, as financial engineers are known, had begun pointing to warning signs years ago. But while markets were booming, the incentives on Wall Street were to keep chasing profits by trading more and more sophisticated securities, piling on more debt and making larger and larger bets.

"Innovation can be a dangerous game," said Andrew W. Lo, an economist and professor of finance at the Sloan School of Management of the Massachusetts Institute of Technology. "The technology got ahead of our ability to use it in responsible ways."

That out-of-control innovation is reflected in the growth of securities intended to spread risk widely through the use of financial instruments called derivatives. Credit-default swaps, for example, were originally created to insure blue-chip bond investors against the risk of default. In recent years, these swap contracts have been used to insure all manner of instruments, including pools of subprime mortgage securities.

These swaps are contracts between two investors—typically banks, hedge funds and other institutions—and they are not traded on exchanges. The face value of the credit-default market has soared to an estimated \$55 trillion.

Credit-default swaps, though intended to spread risk, have magnified the financial crisis because the market is unregulated, obscure and brimming with counterparty risk (that is, the risk that one embattled bank or firm will not be

able to meet its payment obligations, and that trading with it will seize up).

The market for credit-default swaps has been at the center of the recent Wall Street banking failures and rescues, and these instruments embody the kinds of risks not easily captured in math formulas.

"Complexity, transparency, liquidity and leverage have all played a huge role in this crisis," said Leslie Rahl, president of Capital Market Risk Advisors, a risk-management consulting firm. "And these are things that are not generally modeled as a quantifiable risk."

Math, statistics and computer modeling, it seems, also fell short in calibrating the lending risk on individual mortgage loans. In recent years, the securitization of the mortgage market, with loans sold off and mixed into large pools of mortgage securities, has prompted lenders to move increasingly to automated underwriting systems, relying mainly on computerized credit-scoring models instead of human judgment.

So lenders had scant incentive to spend much time scrutinizing the credit-worthiness of individual borrowers. "If the incentives and the systems change, the hard data can mean less than it did or something else than it did," said Raghuram G. Rajan, a professor at the University of Chicago. "The danger is that the modeling becomes too mechanical."

Mr. Rajan, a former chief economist at the International Monetary Fund, points to a new paper co-authored by a University of Chicago colleague, Amit Seru, "The Failure of Models That Predict Failure," which looked at securitized subprime loans issued from 1997 to 2006. Their research concluded that the quantitative methods underestimated defaults for subprime borrowers in what the paper called "a systematic failure of default models."

A recent paper by four Federal Reserve economists, "Making Sense of the Subprime Crisis," found another cause. They surveyed the published research reports by Wall Street analysts and economists, and asked why the Wall Street experts failed to foresee the surge in subprime foreclosures in 2007 and 2008. The Fed economists concluded that the risk models used by Wall Street analysts correctly predicted that a drop in real estate prices of 10 or 20 percent would imperil the market for subprime mortgage-backed securities. But the analysts themselves assigned a very low probability to that happening.

The miss by Wall Street analysts shows how models can be precise out to several decimal places, and yet be totally off base. The analysts, according to the Fed paper, doggedly clung to the optimists' mantra that nominal housing prices in

the United States had not declined in decades—even though house prices did fall nationally, adjusted for inflation, in the 1970s, and there are many sizable regional declines over the years.

Besides, the formation of a housing bubble was well under way. Until 2003, prices moved in line with employment, incomes and migration patterns, but then they departed from the economic fundamentals.

The Wall Street models, said Paul S. Willen, an economist at the Federal Reserve in Boston, included a lot of wishful thinking about house prices. But, he added, it is also true that asset price trends are difficult to predict. “The price of an asset, like a house or a stock, reflects not only your beliefs about the future, but you’re also betting on other people’s beliefs,” he observed. “It’s these hierarchies of beliefs—these behavioral factors—that are so hard to model.”

Indeed, the behavioral uncertainty added to the escalating complexity of financial markets help explain the failure in risk management. The quantitative models typically have their origins in academia and often the physical sciences. In academia, the focus is on problems that can be solved, proved and published—not messy, intractable challenges. In science, the models derive from particle flows in a liquid or a gas, which conform to the neat, crisp laws of physics.

Not so in financial modeling. Emanuel Derman is a physicist who became a managing director at Goldman Sachs, a quant whose name is on a few financial models and author of *My Life as a Quant—Reflections on Physics and Finance* (Wiley, 2004). In a paper that will be published next year in a professional journal, Mr. Derman writes, “To confuse the model with the world is to embrace a future disaster driven by the belief that humans obey mathematical rules.”

Yet blaming the models for their shortcomings, he said in an interview, seems misguided. “The models were more a tool of enthusiasm than a cause of the crisis,” said Mr. Derman, who is a professor at Columbia University.

In boom times, new markets tend to outpace the human and technical systems to support them, said Richard R. Lindsey, president of the Callcott Group, a quantitative consulting group. Those support systems, he said, include pricing and risk models, back-office clearing and management’s understanding of the financial instruments. That is what happened in the mortgage-backed securities and credit derivatives markets.

Better modeling, more wisely applied, would have helped, Mr. Lindsey said, but so would have common sense in senior management. The mortgage securities markets, he noted, grew rapidly and generated high profits for a decade. “If

you are making a high return, I guarantee you there is a high risk there, even if you can't see it," said Mr. Lindsey, a former chief economist of the Securities and Exchange Commission.

Among quants, some recognized the gathering storm. Mr. Lo, the director of M.I.T.'s Laboratory for Financial Engineering, co-wrote a paper that he presented in October 2004 at a National Bureau of Economic Research conference. The research paper warned of the rising systemic risk to financial markets and particularly focused on the potential liquidity, leverage and counterparty risk from hedge funds.

Over the next two years, Mr. Lo also made presentations to Federal Reserve officials in New York and Washington, and before the European Central Bank in Brussels. Among economists and academics, he said, the research was well received. "On the industry side, it was dismissed," he recalled.

The dismissive response, Mr. Lo said, was not really surprising because Wall Street was going to chase profits in the good times. The path to sensible restraint, he said, will include not only better risk models, but also more regulation. Like others, Mr. Lo recommends higher capital requirements for banks and the use of exchanges or clearinghouses for the trade of exotic securities, so that prices and risks are more visible. Any hedge fund with more than \$1 billion in assets, he added, should be compelled to report its holdings to regulators.

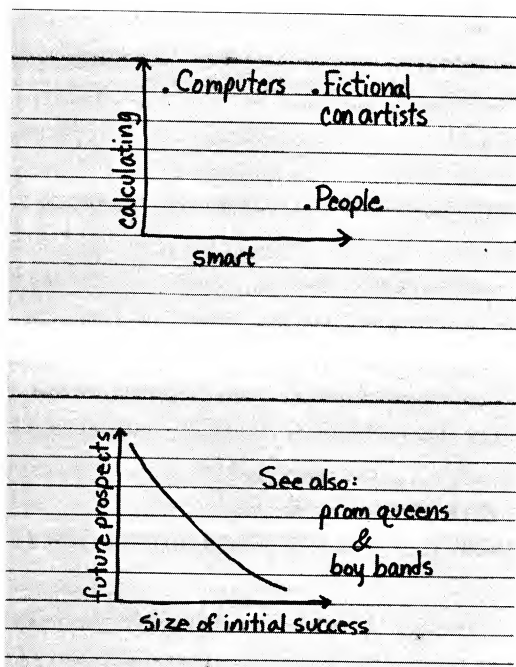
Financial regulation, Mr. Lo said, should be seen as similar to fire safety rules in building codes. The chances of any building burning down are slight, but ceiling sprinklers, fire extinguishers and fire escapes are mandated by law.

"We've learned the hard way that the consequences can be catastrophic, even if statistically improbable," he said.

November 4, 2008

Playing the Odds

By GEORGE JOHNSON



State lotteries, it's sometimes said, are a tax on people who don't understand mathematics. But there is no cause for anyone to feel smug. The brain, no matter how well schooled, is just plain bad at dealing with randomness and probability. Confronted with situations that require an intuitive grasp of the odds, even the best mathematicians and scientists can find themselves floundering.

Suppose you want to calculate the likelihood of tossing two coins and coming up with one head.

The great 18th-century mathematician Jean Le Rond d'Alembert thought the answer was obvious: there are three possibilities, zero, one or two heads. So the odds for any one of those happening must be 1 in 3.

But as Leonard Mlodinow explains in *The Drunkard's Walk: How Randomness Rules Our Lives*, there are, in fact, four possible outcomes: heads-heads, heads-tails, tails-heads and tails-tails. So there is a 25 percent chance of throwing zero or two heads and a 50 percent chance of throwing just one. In the long run, anyone offering d'Alembert's odds in a coin-flipping contest would lose his shirt.

The key to puzzles like this, Mlodinow writes, is Cardano's method, named for Gerolamo Cardano, author of the 16th-century *Book on Games of Chance*. To lay the odds for even the simplest-seeming event, one constructs a table, or "sample space," of all the ways Fortuna's dice might fall. Trust your instincts instead and you're bound to go wrong.

If a woman has two children and one is a girl, the chance that the other child is also female has to be 50-50, right? But it's not. Cardano again: The possibilities are girl-girl, girl-boy and boy-girl. So the chance that both children are girls is 33 percent. Once we are told that one child is female, this extra information constrains the odds. (Even weirder, and I'm still not sure I believe this, the author demonstrates that the odds change again if we're told that one of the girls is named Florida.)

Mlodinow—the author of *Feynman's Rainbow*, *Euclid's Window* and, with Stephen Hawking, *A Briefer History of Time*—writes in a breezy style, interspersing probabilistic mind-benders with portraits of theorists like Jakob Bernoulli, Blaise Pascal, Carl Friedrich Gauss, Pierre-Simon de Laplace and Thomas Bayes. The result is a readable crash course in randomness and statistics that includes the clearest explanation I've encountered of the Monty Hall Problem (named for the M.C. of the old TV game show *Let's Make a Deal*).

You are presented with three doors, behind one of which is a new car. You take your pick, but before your fate is revealed, the M.C. swings open one of the other doors, revealing a booby prize.

So far, so good, but now comes the big decision. Do you stay with your original choice or switch to the other unopened door? Even the great mathematician Paul Erdos was dumbfounded to realize that this is not a 50-50 proposition. If you lay out the possibilities on Cardano's grid, you will see that your odds actually improve if you change doors.

The key to this puzzle is that the door the M.C. opens is not chosen at random. (He's not going to ruin the game by prematurely revealing the car.) As in the two-daughter problem, the additional information skews the odds, and with Cardano's method you can make a rational, though counterintuitive, decision.

In all these cases, people err by assuming a situation is more random and unconstrained than it really is. More often we make the opposite mistake: overestimating the amount of control we have over life. Mlodinow tells the story of a Paramount executive, Sherry Lansing, who presided over the company's motion picture group during a string of blockbusters: *Forrest Gump*, *Braveheart* and *Titanic*. She was hailed in the Hollywood press as a genius, until she suddenly lost her touch. After a series of box-office disasters, she was replaced. The studio appeared to be justified in its decision when it went on to have its best summer in a decade.

But not so fast, Mlodinow cautions. More recent winners, *War of the Worlds* and *The Longest Yard*, were in production when Lansing was still in charge. Like

so many things in life, the success or failure of a movie is heavily influenced by factors beyond anyone's control. Fortunate events like a string of hit movies are most likely to be followed by more ordinary events. Lansing, Mlodinow writes, was a victim of what statisticians call regression toward the mean.

Anyone who has ever bought a mutual fund because it has been on a roll or bet that a racehorse will extend its winning streak has fallen into the same confusion. Chances are the champion will regress toward the mean and another will have its glory day. In all life's games, some players are better than others, but randomness maintains the upper hand.

Hardest of all for our blinkered brains are cases involving Bayesian statistics, where one must gauge how the probability of one event hinges on that of another. Mlodinow learned the difficulty firsthand nearly 20 years ago when his doctor told him, out of the blue, that it was 99.9 percent certain that he was infected with H.I.V. Mlodinow had none of the risk factors (except for being human), but he had scored H.I.V.-positive on a test that had a false positive rate of 1 in 1,000.

If his doctor had studied probability in medical school, he would have seen the situation in a different light. Statistics from the Centers for Disease Control and Prevention showed that in Mlodinow's demographic group, 1 in 10,000 people tested positive and was ultimately confirmed as carrying the virus. In addition, there were the statistical flukes—the 10 (1 in 1,000) who were false positives. Compare those numbers, and the chance that Mlodinow was infected (he wasn't) was 1 in 11.

When statistics are used in a court of law the effect can be just as misleading. Mlodinow recalls the O. J. Simpson trial, in which the prosecution depicted the defendant as an inveterate wife abuser. One of Simpson's lawyers, Alan Dershowitz, countered with statistics: in the United States, four million women are battered every year by their male partners, yet only 1 in 2,500 is ultimately murdered by her partner.

The jury may have found that persuasive, but it's a spurious argument. Nicole Brown Simpson was already dead. The relevant question was what percentage of all battered women who are murdered are killed by their abusers. The answer, Mlodinow notes, didn't come up in the trial. It was 90 percent.

Lawyers, it seems, are no better than doctors at this kind of math. But juries are even worse.

June 8, 2008

Monday Puzzle: Solution to Birthday Problem

By PRADEEP MUTALIK

From July 4th to Labor Day, we've had a breathless succession of well-discussed puzzles. Now we're going to explain solutions and award prizes. In order to concentrate on solutions this week, we're not having a new puzzle today, but the discussion of Justin Thyme's brilliant Slippery Slope Jewelry puzzle from last week is still very much alive.

Several readers have suggested that they'd like to see mathematical principles involved in solving puzzles explained. We'll try to do this as best we can in the context of puzzle solutions. We are fortunate in this blog to have some brilliant regular commenters who are not only great puzzle solvers but very good explainers and extremely helpful souls as well: take a bow D-Ferg, Tom E. and Andrew M! We'll reference the well-thought-out explanations of these and other contributors and then address specific questions or requests to explain things that you may have.

In today's column, I want to illustrate two things: first, a different way in which probability problems can be approached; and second, how even tough problems involving probability can be tackled by first thinking about a "toy" version of them. So here goes! In analyzing the puzzle Happy Birthday, America, we are going to dive boldly into the deep end. We are going to go step by step through the problem of determining how many people need to be in a group before there is an even chance or greater that three of them will share a birthday. Don't worry, we'll take it slowly, so follow carefully. This problem is tough, no doubt, but once you master it, you'll hopefully have the confidence to be able to tackle a great variety of probability problems. (You can check out the answer to the simpler problem involving two people sharing a birthday later in this column.)

I had outlined a simple approach to problems involving probability in the solution to The Lady and the Toaster. You just articulate, in plain English, all the ways that a certain result can be achieved and multiply the probabilities of the individual events whenever you use an "and" and add them when you use an "or."

This approach can always be applied (I always use it in toy versions of large problems to check my results), but the calculations resulting from it can get unwieldy in a problem as big as this. So, we need to bring out the heavy artillery—combinatorics. Does this bring back some fuzzy memories of formulas

for permutations and combinations from high school? What are these entities which are so easy to mix up, and when do you use which formula? Here's a simple rule that's pretty much all you need to carry in your head (it helps to remember the formulas too, but you can always look them up): When you have to *choose*, use combinations; when you *arrange* or *order*, use permutations! That's all there is to it! Our tough problem basically uses just one permutation, two combinations, and a simple summation. The trick is to keep each calculation separate from others, and use the right numbers for each.

In this approach to probability problems, we try to imagine the entire universe of possibilities: what is known as the *sample space*. Imagine all those gazillions of groups of n people standing in a row, representing every possible case. Now try to enumerate the groups that interest us (or the ones that don't interest us, if that's easier!). We then divide the groups of interest by the total number of groups in the entire sample space and we have our probability. In the case of the three coincident birthdays problem, it is easier to list the groups that don't interest us. If we can find the relevant numbers—the number of groups with no pairs of people with shared birthdays, the number of groups with exactly one pair, the number with exactly two pairs and so on, up to the maximum number of pairs possible—and add them all up, we will be able to calculate the probability of *not* having three or more people with shared birthdays. If we subtract this probability from one, we will have our answer.

Okay, we have our strategy, but the numbers here are daunting (for 50 people, the entire sample space is 365^{50} different groups) and it is easy to get confused. So let's think about a toy version of the problem, with just enough complexity to help us reason about the larger problem. We want to allow for at least two pairs, so let's consider five people. And instead of people sharing birthdays, let's just determine the probabilities of their being born in the same quarter of the year.

That's much better! We have five people, each of whom can be born in one of four quarters, so the total universe of groups is 4^5 or 1,024 (the first person could be born in any of four quarters, the second could be born in any of four and so on). Now let's consider how many of these groups have exactly two pairs sharing birth quarters. For a moment, imagine that you've already chosen the five people and their birth quarters are Q1, Q1, Q2, Q2 and Q3. You would have had the exact same result if you had picked them in a different order like Q1, Q2, Q1, Q2 and Q3. Each of these is a single group in our universe, and must be counted. We need to determine all the possible arrangements of two identical pairs in a

group of five. We are *arranging*, so we use—you've guessed it, permutations! But before we use any formula, let's calculate it by hand using the letters a, b and c to represent Q1, Q2 and Q3. We have to find all possible arrangements of the letters aabbc. The c could be in any of five positions, and there are six possible arrangements for aabb: aabb, abab, abba, baab, baba and bbaa. So the total is $5 \times 6 = 30$. If our formula doesn't give us 30, we'll know that what we're using is wrong. Actually, the formula we need to use here is a simple and powerful one that's a joy to use. It's the formula for permutations from a multiset (also known as the multinomial coefficient) and is simply $5!/2!2!$ which, correctly, gives 30. Take the factorial of the total number in the group and divide it by the factorials of the numbers of all the groups that have repeats ($n!/a!b!c!\dots$). This formula is really handy in permutation problems. The classical example is how many arrangements can you make of the letters in the word MISSISSIPPI. There are 11 letters, with three repeated letters: four Ss, four Is and two Ps. So the answer is $11!/4!4!2!$ which is 34,650. If there were no repeats, the answer would be just $11!$ which is about 40 million.

Okay, we've got the permutation nailed. But we had assumed that we already had Q1, Q1, Q2, Q2, and Q3 picked. Instead of Q1 and Q2, we could have chosen any two different quarters, so we need to multiply the 30 arrangements we got by the number of ways we could choose two different quarters out of four. *Choosing*, so use combinations! The formula for this is $4!/2!2! = 6$ (${}_nC_r = n!/r!(n-r)!$ where n is the total number you choose from, and r is the number you pick). Finally you have to multiply by the number of ways you could have picked the lone person who was not part of a pair. After you take away the two pairs, there are two quarters left and you could pick any one of them, so the number of ways is $2!/1!1! = 2$. Multiplying all these together, you get $30 \times 6 \times 2 = 360$ distinct groups having exactly two pairs out of the total universe of 1,024 groups, giving a probability of $360/1,024$ or 35.2%.

That's it! We've gone through all the exact same steps we would need to solve the tough problem of three coincident birthdays. Let's set it up in an Excel spreadsheet. We'll first do it for 88 persons, which we know is the right answer, thanks to this paper by Diaconis which was referred to by PK. We can do the calculation in one humongous formula, but I'm going to do it in several steps: it's easier to understand and more flexible.

Let's leave the top two rows for titles. In Column A, we're going to have the number of people in the group, so type "88" in cell A3, and then drag-fill all the

cells from A4 through A47 with it (to drag-fill, select A3, grab the + shaped cursor at the lower-right corner of the selected cell(s) and drag it to A47). In Column B, we're going to have the number of pairs, so fill B3 to B47 with the numbers 0 through 44, since 44 is the largest number of pairs of people sharing birthdays in a group of 88. An easy way to do this is to put 0 in B3, 1 in B4, select these two cells and drag-fill to B47. In Column C, we calculate all the arrangements of groups having the number of pairs in the Column B cell for that row, so fill C3 with the following formula (you can copy it from here): $=\text{FACT}(A3)/((\text{FACT}(2))^{B3})$, and drag-fill through C47. In Column D are the ways of choosing the number of pairs. In D3, type in or copy $=\text{COMBIN}(365, B3)$ and drag-fill to D47. In Column E are the ways of choosing the remaining people that don't share birthdays: $=\text{COMBIN}(365-B3, A3-2*B3)$. Drag-fill to E47. In Column F, we put in the total universe of groups in the sample space: $=365^{A3}$. Drag-fill to F47. Finally in Column G, we calculate the probability for each number of pairs by multiplying the 1 permutation and 2 combinations together and dividing by the total universe. Type in $=(C3*D3*E3)/F3$ into G3 and drag-fill to G47. Now add up the cells in Column G and we have our probability for having any of 0–44 pairs. If you did this correctly you will get 0.4889. So the probability for having at least one triplet of people sharing a birthday is $1 - 0.4889 = 0.511$, just slightly above even. Scanning the spreadsheet gives us some other interesting information. In a group of 88, the most probable number of shared-birthday pairs is eight, followed by nine: both likely to happen about 8% of the time. Second, you can see that the universe of possible groups in Column F is humongous, approximately three followed by 225 zeroes. This is close to the limit of what Excel can calculate.

You can copy the entire block of cells from B3 through G46 elsewhere in the spreadsheet, and change all the 88s in the first column to 87s. This gives the probabilities for having 0–43 pairs (43 pairs is the maximum for 87) in a group of 87 people. The sum comes out to be 0.5005, implying a 0.4995 probability of having at least one triplet. This is pretty darn close to 50%, but misses it by a whisker. So here's something to think about. We have not considered the case of people born on Feb. 29 in leap years. Had we done so, how would it have affected the probability for triplets in a group of 87: would it have pushed it over 50% or would it have pushed it in the other direction? I leave it to you to ponder that.

Let's consider the other problems in the Happy Birthday puzzle. We started with statistical significance.

Let's say a friend challenges you to a coin-tossing game: multiple rounds, a dollar a round. He pulls a coin out of his pocket and says, "Heads I win, tails you do." You go along. The coin lands up heads, you lose. Never mind, you think, my turn will come. It's heads again. And again. And again. At what point do you say to yourself, "There's something fishy going on here. Maybe this is not a fair coin." This is the idea behind statistical significance.

We know that sometimes lucky—and unlucky—streaks occur by chance. So we have all learned to tolerate some degree of improbability, attributing it to just coincidence. At some point however, you have to say, "Enough is enough! I have to investigate this. There may be something else going on." If you keep investigating everything that is even the slightest bit unlikely, you will find yourself involved in many futile goose chases. On the other hand, if you are never spurred to look deeper, you will miss genuine phenomena. What is the optimal point, the statistical version of "reasonable doubt"? The point that has been accepted, arbitrarily, in most of the world of science, is 5%. If the likelihood that something will happen just by chance is less than 1 in 20, scientists assume that there is probably some genuine non-random process going on. Extremely sophisticated statistical procedures, called tests of significance, have been developed to quantify the likelihood of a particular result. Very few phrases can excite a researcher more than to hear the magical phrase " $p < 0.05$," meaning that his or her result has a lower than 5% probability to have occurred by chance.

In the puzzle, I mentioned that our July 4th party had 21 guests, out of which one had a July 4th birthday. Was this statistically significant? As Tom E. nicely showed, the probability of this was about 5.6%. So, I would be justified in letting this pass. Had there been 2 people who both had birthdays on July 4, I would have been justified in getting suspicious and investigating. Maybe my wife was purposely selecting those of our acquaintances that had July 4th birthdays. Or it could still have been a coincidence—just an extremely unlikely one. But because it would be unlikely, I would not have to investigate too many such instances.

One such instance that definitely calls for investigation is historical instance of John Adams, Thomas Jefferson and James Monroe all dying on July 4th. As Tom E. points out, the probability of this is 1 in 5 million, certainly far beyond statistical significance: even one of the first five presidents passing away on July 4th would have been remarkable. As Justin Thyme remarked, we need to consider sample size here. When the sample size is small, the statistical fluctuations can

be large. These get smoothed out as the sample sizes get larger. For U.S. presidents, we now have a sample size of 38. No other presidents have passed away on July 4th. If we perform the probability calculation for 38, it comes out to be 5.8%: which would not be significant if the day was any old day. But the fact that renders it significant still, is that July 4th is the most important day in American history! So, three out of 38 presidents passing away on July 4th is significant. Was there something else going on? I had suggested a hypothesis that in their last days, humans can hold on to life by sheer force of will so that they can reach a particular landmark date or occasion one last time. To actually see if this is plausible, we need to examine the actual circumstances of their deaths. If they died due to accidents, or were not aware of the date, then obviously their will was not involved. Well, in case of the three presidents, they were probably lucid, and in fact John Adams is reported to have said on the day of his death, "It is a great day. It is a good day." So the theory is plausible, but we must guard against the possibility that we are selecting this sample of people after the event. After all, there are also sick people who had every reason to extend their life a small amount, but who didn't make it—a recent example being President Obama's grandmother who passed away the day before the historic election that made him president. To actually prove or disprove such a theory would require a rigorous scientific study involving, first, a large number of people at roughly the same stage of terminal illness. In each case, we would have to know beforehand that they were trying to hold on to life up to a particular date approximately the same number of days in the future. To absolutely clinch it, one would have to discover the physiological mechanism (adrenaline, etc.) that the body employed to cling on to life. A pretty difficult research project to conduct, by any means!

Finally, Tom E. nicely explained the answer to the classical birthday problem and our variation here and here. The answer to the first problem—what is the smallest number of people in a group such that there is an even chance or greater that two of them will share a birthday—is 23. And the size of the group that gives an even chance or greater that two people will have a birthday within a day of each other is a mere 14. These numbers are indeed very small, much smaller than what most people intuitively expect. A group of 14 is just three average-size families on a weekend get-together. No wonder we are struck by wondrous coincidences: they are mathematically far more likely than we expect.

For his many contributions, Tom Enrico from Sandy, Utah, gets the prize for this puzzle and becomes our third multiple prize winner (he had previously won

a prize for the DeCAPitated puzzle). Congratulations, Tom. Tom will receive a second puzzle-related book.

Finally, a word about Persi Diaconis, the author of the paper cited above, who is the third mathematician to be mentioned in these columns who also happened to be a stage magician. Diaconis has also been a very active skeptic, who in his career has debunked a lot of tall tales and false beliefs. Another stage magician who was also a famous skeptic was James ("The Amazing") Randi. Perhaps stage magicians can clearly see how gullible people are, how easily they can be fooled and how easily legends of miracles and the supernatural can be created. When they are also adept at mathematics, like Persi Diaconis, it is easy for them to see that the coincidences that people make so much of—as this recent *Times* article did—are not remotely as unlikely as people believe them to be. Do people who believe in the supernatural do so because they are bad at estimating probabilities? There's probably some truth to this, but that's a subject for another, very likely to be extremely controversial, column.

September 7, 2009

Just What Are Your Odds in Genetic Roulette? Go Figure

By GINA KOLATA

My father is not an optimistic person, but he certainly had a rosy view of the life expectancies in his family. Everyone, he always said, lived into their late 80s or even their late 90s, and died, not of a specific disease, but of "old age." My mother said her family was equally long-lived. Naturally, my sisters and I grew up thinking that we were genetically blessed.

Then one day it hit me. My parents were eliminating a few close relatives from their data set. What about my father's brother who died when he was in his early 20s after a botched tonsillectomy? Or the brother who died of trauma while he was still a young man? How about my mother's mother, who died of asthma as a young woman? They did not count, my father said, since today their deaths would not have occurred. What about my aunt who had multiple medical problems? She smoked and did not take care of herself, my mother explained.

Now, no longer sure that I have a long and healthy old age to look forward to, I peer at my parents as they grow old and wonder what will be my fate. Can you change the genetic roulette? Will all those years of exercise and weight lifting prevent me from shrinking a few inches in height? Will frequent tests for Paget's disease, a degenerative bone disorder, help me to detect it early, if I get it, and avoid the hearing loss that has plagued my father? How much of our future is in our own hands, or the hands of medical researchers avidly looking for causes and cures of illnesses, and how much was predetermined at birth?

My children, meanwhile, are looking at my husband and me and seeing their personalities and their futures. My daughter thinks she inherited her exuberance from me. My son is convinced that his reserve was a bequest of his father. I told my daughter that my cholesterol levels were getting out of control. Oh, no, she said, that means it will happen to her.

In a way, it is irresistible, this fixation on genetic predestination—especially when evidence can be seen in the mirror. But as my father's view of his family's longevity demonstrated, it can be deceptive.

Remember the Jim twins? They were the subjects studied a decade ago by Thomas Bouchard of the University of Minnesota. Identical twins reared apart, they both just happened to be named James—James Lewis and James Springer.

Each just happened to marry and divorce women named Linda, then remarry women named Betty. The Jim twins named their dogs Toy and their firstborn sons James Alan and James.

Could genes really be so controlling? Not exactly, say statisticians. It is a classical example of the multiple end-point problem, something that undoubtedly is prompting all of us to give more weight to genetics than is warranted. The difficulty is that there are hundreds of thousands of traits that any two people can share, and if you look at any two people plucked randomly, you are sure to find that they have one or two traits in common, independent of genetics. If both Jim twins had not been named Jim, they both might have worn wire-rimmed glasses or lived on streets named Elm Road, for example.

"There are endless possibilities for doing bad statistical inferences," said Persi Diaconis, a statistician at Stanford University. And when we look at our parents, or our children, and see ourselves, it is easier than we think to get caught in the multiple end-points statistical trap.

Of course, we also have an urge to see what we want to see in our relatives, and the multiple end-points problem lets us do it with abandon. "You get to pick which features you want to resonate to," Professor Diaconis said. "When you look at your mom, you might say, 'I'm exactly the opposite.' Someone else might say, 'Hmm.'"

Yet the more scientists learn about particular genes, the more they can tell us what is inherited from our ancestors. The focus is on disease, which is, after all, the legacy that can change our lives the most. Instead of looking at a mosaic of personality traits as well as appearances, talents and diseases that seem to run in families, many geneticists are stalking tiny variations in the genetic blueprints of individuals that can say whether a disease will show up in the future. Or, most commonly, they are seeking genetic variations that will tell us whether we have a predisposition to a disease. Whether we get the disease may depend on how well we take care of ourselves or whether scientists can develop drugs to prevent the disease for those who are susceptible. Or it may depend on blind luck. But with the emerging plethora of genetic information, the question now is, How much do we want to know?

Dr. Allen Roses, who is the vice president and worldwide director of genetics at the giant pharmaceutical company GlaxoWellcome, does not yet know the genetic variations that shaped his medical history, but he is pursuing them with a sense of personal mission. At age 46, he knew he might be susceptible to

heart disease, even though his cholesterol level was normal. He looked at his family—his father, mother and sister had had heart attacks, although they also had normal cholesterol levels. So, to keep his heart in top condition, he taught aerobics classes.

"I was in the best shape of my life," Dr. Roses said. "Except I had a heart attack."

Now, armed with new techniques of molecular genetics, Dr. Roses is directing research that looks for genetic variations that predispose people to heart attacks at an early age, people who, like himself, have normal cholesterol levels. He fervently thinks that once he finds the genetic footprints for this susceptibility, his company will find drugs to help others and himself. "We want the drug that's going to work," Dr. Roses said.

For Charles P. Pierce, a writer-at-large for *Esquire* magazine, the new genetic research forced him to confront a troubling question: Did he want to know whether he, like his father and his father's four brothers, would develop Alzheimer's disease? He wanted to think that the disease was not in the genes; that way, he could avoid the weight of the past generation's experiences. Clinging to the now-discredited idea that Alzheimer's disease is caused by aluminum, he reminded himself that his father had been exposed to aluminum during World War II on Navy ships.

"The most prolonged exposure I had to aluminum was wrapping the leftovers in foil after dinner," Mr. Pierce wrote in his forthcoming book, *Hard to Forget: An Alzheimer's Story*. "If it was aluminum, I was safe." Then he spoke to a scientist who told him bluntly: "The idea is that you don't get Alzheimer's disease from aluminum. You get it from bad genes."

Now scientists have found a handful of genes that can lead to Alzheimer's disease. The question for Mr. Pierce is, Should he be tested to find out if he has one of them?

He has decided not to after speaking to a doctor who told him: "When it comes to being tested, I always point out that there has to be some reason to be tested. If you believe that you'd live your life differently, then there might be some reason to be tested." With no way of preventing the disease, and the fear of genetic discrimination lurking, Mr. Pierce thinks he is better off not knowing.

"The one thing that was remarkable to me is that the scientists are throwing this stuff way out ahead of the legal system, cultural mores, all kinds of things," Mr. Pierce said in a recent interview. "I'm not sure we've done enough to catch up."

Dr. Roses differs. "In fact, we're not moving fast enough because we don't have the kinds of treatments we need," he said. Take his own genetic curse, the heart attack at a young age.

"Half of the people who have these early heart attacks die," Dr. Roses said. "There are a lot of people dying because we aren't moving fast enough."

March 8, 2000

The 2000 Election: The Science of Counting

By GINA KOLATA

First George W. Bush led Al Gore by 1,784 votes in Florida. Then, an unofficial count by the Associated Press suggested his lead was slashed to less than half that. So, which number is right mathematically?

Statisticians chuckled at the idea.

"There's always going to be an error," said Howard Wainer, a statistician at the Educational Testing Service in Princeton, N.J. "Every time you count them, you're going to get a different answer."

In research, said Diana C. Mutz, a professor of political science at Ohio State University, scientists will repeat a process multiple times and choose a number somewhere in the middle of their data as most likely to reflect the truth. But, she and others said, multiple recounts are probably not desirable in the presidential election because they would add to the delay and uncertainty—not to say the bickering. Whoever was losing could argue for one more recount.

Even if it were just a research question, Professor Mutz was not sure how many counts would be needed to make her confident the Florida vote was as accurate as it could be. How many times she would count it "depends on how many graduate students I have," she joked.

Then there is the problem of Palm Beach County, Fla., where residents said confusion over the ballot led more than 19,000 voters in a heavily Democratic area to mark two candidates instead of one for president. Their ballots were discarded as invalid. And, adding to the confusion, Patrick J. Buchanan won more than 3,000 votes in Palm Beach. Some Democrats said many people accidentally voted for Mr. Buchanan when they meant to vote for Mr. Gore. Isn't there a way to fix that? A statistical adjustment, perhaps?

Sorry, say the statisticians. Any adjustment would only make matters worse. Persi Diaconis, a statistician at Stanford University, said the situation reminded him of attempts to adjust the census to correct for the undercount, the people who were missed. The census recount turned out to be a nightmare, he said, with new errors introduced and even more squabbling.

"The process really degenerates," Professor Diaconis said. "It's not at all simple."

November 10, 2000

Prospectus; Can a Computer Program Figure Out the Market? A Former Analyst and a Mathematician Are Betting That Theirs Can

By JANET STITES

Silicon Alley in New York is known for many things, but not as a hotbed for advances in computer science.

Mention genetic algorithms or artificial intelligence, common parlance among computer scientists, and eyes may very likely roll among even the most respected new-media executives in New York. In fact, an almost Luddite attitude toward hard technology seems to prevail in Silicon Alley, where Bikini.com, "the world's biggest beach party," is an example of the cutting edge.

On the fringes of Silicon Alley, though, can occasionally be found a company like the Intelligenes Corporation, which was founded in early 1997 by Ben Goertzel, a mathematician, and Lisa S. Pazer, a former Wall Street economist and analyst. Intelligenes is trying to change the way people measure business risks or make buying decisions by combining, in a software program called Webmind, elements of the Internet with artificial intelligence technology or "machine learning," by which the software can, for example, "remember" who Alan Greenspan is and why he matters.

The technology is the brainchild of Dr. Goertzel, who received his Ph.D. in mathematics at age 22 from Temple University, then did research at the University of Western Australia and later taught mathematics, computer science and psychology at City University of New York.

"For a long time, I had been designing an architecture for artificial intelligence, but didn't have the machine to do it on," said Dr. Goertzel, now 32. "When I started using the World Wide Web, I realized it was a metaphor for the brain—that the Web could be a mind."

Webmind gathers and processes what it perceives as "human intelligence" data from text documents, like news articles—whether on the Internet or corporate networks—to help users spot trends or make predictions. The results, which can be presented as numbers, a chart or perhaps eventually even a sentence, are

meant to complement rather than replace traditional mathematical modeling—to help analysts, in a sense, to read between the lines.

Ms. Pazer herself left off trying to outguess Mr. Greenspan, the Federal Reserve chairman, and quit Wall Street in 1993 to write a novel. But after coming across Dr. Goertzel's research on the Web, she put aside her fiction project to start *Intelligence*, which she now serves as president and chief executive.

Here is how she explains Webmind: "If you want to try to determine whether Greenspan is likely to raise interest rates, Webmind can query news archives for Greenspan's comments over the last six months. Because it understands aspects of natural language, it can give a qualitative answer by building a graph giving weight to each of his comments and showing how he reacted in the past in relation to his comments. You don't search for documents; you search for answers."

At full throttle, the software is supposed to be able to answer specific queries that depend on establishing relationships, like "How much money did the United States give to Russia in 1998?"

Ms. Pazer contends that Webmind has far-reaching applications. "The financial market is our proving ground," she said. "We can measure risk and volatility. But the technology could be used by anyone trying to evaluate risk or isolate trends." The list of potential users ranges from risk managers at insurance companies to market researchers to political strategists.

But Webmind is still in its infancy. *Intelligence* is currently testing the software with potential customers and has a demonstration for qualified users at its Web site, www.intelligence.net. "We have to prove to them that the technology works," Ms. Pazer said.

If they do that, Dr. Goertzel and Ms. Pazer hope to develop partnerships, supplying Webmind to financial news services or other online information providers, in a revenue-sharing arrangement. As the Webmind brand becomes more established, Ms. Pazer would look for such partnerships to give way to straight licensing deals.

Though the business viability of *Intelligence*'s product remains to be seen, the company has attracted the involvement of some influential people.

The vice chairman, for example, is John B. Evans, a co-founder and chairman of another Alley-based company, Biztravel.com. Danny Hillis, co-founder of the supercomputer company Thinking Machines, who is now vice president of research and development in the Walt Disney Company's department of imagining, recently joined the *Intelligence* strategic advisory board.

Among others who are watching the progress of Webmind is Alexander Chislenko, a researcher at the Media Lab at Massachusetts Institute of Technology who has followed Dr. Goertzel's work for some time, because it complements some of his own. "I think it's a credible technology, and the approach is promising," Mr. Chislenko said. He predicted that Webmind would prove valuable in modeling some parts of the financial market that other technologies cannot. But Mr. Chislenko cautioned, "No technology can predict the whole market."

Backed solely by private investors so far, Intelligenesis employs nearly 30 people, with a heavy mix of programmers trained in the social sciences—some working from the company's office on Lower Broadway, others commuting by way of the Internet from Norway, Russia, Brazil and Australia.

Dr. Goertzel and Ms. Pazer contend that all the really significant predictions and decisions that people make are, in the end, based on human psychology. And Webmind, they say, can use artificial intelligence to translate the multitudinous outpourings of human psychology into valuable data.

"When you think about Webmind, think about being at a cocktail party," Ms. Pazer said. "Think if you could process not just the conversations you had, but all the conversations in the room."

February 8, 1999

New Tools for the I.R.S. to Sniff Out Tax Cheats

By DAVID CAY JOHNSTON

Been cutting corners on your income tax return? Claiming more in charitable deductions than you gave away? Understating income from your business?

By the middle of the decade, it will probably be much tougher to shortchange Uncle Sam, or state tax agencies, for that matter, than it is today.

At present, a big decline in audits and other enforcement efforts by the Internal Revenue Service, which has suffered from budget cuts and is under orders from Congress to focus on helping taxpayers instead of finding tax cheats, has encouraged many people to play fast and loose with their income tax returns, according to tax professionals and I.R.S. workers.

But the situation could change significantly, thanks to new technology being designed for the I.R.S. to improve service to taxpayers. It can also be used to track known tax cheats and to identify patterns of cheating and fraud. Some states have already acquired a version of the technology and used it with promising results.

The technology, being developed for the I.R.S. by the Computer Sciences Corporation of El Segundo, Calif., will be able to feed data from every entry on every tax return, personal or corporate, through filters to identify patterns of taxpayer conduct. Those taxpayers whose returns suggest that they are highly likely to owe more taxes could then quickly be sorted out and their tax returns audited.

That is not, however, where I.R.S. officials want to focus public attention. The I.R.S. commissioner, Charles O. Rossotti, wants to emphasize improved service to what he calls the I.R.S. customers, and new technology is the key to that goal. And Mr. Rossotti says that, by focusing on helping people who want to comply, the I.R.S. can bring in much more money than by focusing on willful tax avoidance and evasion.

Paul J. Cosgrave, the I.R.S. chief information officer, said that "in our effort to run the I.R.S. more like a business, we are trying to bring in a lot of commercial practices" that are intended to raise more revenue through making compliance easier.

"The main thrust of computer modernization is to help us provide better service," he said.

That said, Mr. Cosgrave acknowledged that the data-mining technology eventually would allow the I.R.S. to find both outright frauds and small-scale cheating. In its current customer-friendly mode, the I.R.S. does not like to call taxpayers cheats because they might cut a few corners.

"We call that stuff 'math errors,'" Mr. Cosgrave said, but, of course, when it finds them it then corrects the "errors" and bills the taxpayers.

The database technology that the I.R.S. will install to track tax returns will be similar in many ways to the databases used by American Express, Citibank and other big credit issuers to decide which charges to approve and which advertisements to slip in the mail with monthly bills. Identifying the behavior patterns of customers is one of the most valuable features of these databases.

In two years or so, the I.R.S. hopes to start building twin databases on each segment of taxpayers, such as salaried workers, small businesses and large corporations. In each segment, one database will be designed to take in revenue rapidly and issue refunds, while the second will compile and store data that can be mined for information by auditors and by customer-service agents helping people at walk-in centers.

And with quick and easy access to data about individual taxpayers, both auditors and tax collectors will be able to identify targets better and spend less time on clerical chores, Mr. Cosgrave said.

The Kansas Revenue Department has already installed a modern computer system based on this type of technology that allows it to look up information on individual taxpayers quickly, often resolving such problems as a lost check by issuing a new one in less than a minute.

But in a few years, once all the kinks are worked out, the system will also be used to look for patterns of cheating, said Pat Compton, a management analyst with the Kansas Revenue Department.

For example, by analyzing sales tax reports from convenience stores, the state could identify enterprises that appeared most likely to be shutting off their cash registers and not paying taxes on every sale.

And in about two years, Mrs. Compton said, the state will be able to resume intense efforts to identify inflated claims for Kansas's property tax rebate. "We have cut back on the scrutiny because of trying to get the new system up and running smoothly, but that is an area where people try to claim the maximum \$600 even if they are entitled to less," she said, "and with our new systems we will be able to identify those people much more easily."

Michael Howard, vice president of data warehousing at the Oracle Corporation, a California software company that sells large database systems, said that by mining its database, a tax authority could find patterns that were not intuitive or obvious.

He said that behaviors that tax authorities traditionally associated with non-compliance might turn out, on analysis of the details in millions of tax returns, to be much less significant than other unseen factors. As an example of the kind of unexpected results data-mining produces, he cited the experience of a telecommunications company that he declined to identify. The company wanted to stem the loss of customers to competitors and, by mining its database, discovered that people who bought its voice mail service rarely defected, a linkage no one had previously noticed. He said the company then decided to give away the voice mail service to retain customers.

Malcolm Sparrow, a Harvard University expert on fraud who is an I.R.S. consultant, has written extensively about how government agencies tend to identify a fraud and then focus increasing resources on it, even as the crooks move on to new frauds. He has urged the I.R.S. to design its database to facilitate hunts for "dynamic fraud," in which the theft technique changes rapidly, but the I.R.S. has made little use of his services, he has said, since Mr. Rossotti was appointed in 1997.

How a database is designed can limit its use as a fraud-detection tool, several database experts said.

Mr. Cosgrave said that "absolutely the way you design your database up front has a lot to do with" its utility as a fraud-detection tool. He said that the creation of the twin databases would go a long way to making the planned new systems useful for fraud detection.

He said detailed decisions at the I.R.S. about how much the new technology would be focused on fraud detection versus customer service were still six to 18 months away.

January 3, 2000



CHAPTER 3

Famous Problems, Solved and As Yet Unsolved

THEY BAFFLED MATHEMATICIANS FOR DECADES, FOR centuries. Many spent years working on them only to give up in despair. Others thought they had solutions, only to be embarrassed when their solutions turned out to be wrong. They are the famous problems of mathematics, and the articles in this section tell some of their stories.

Fermat's Last Theorem was a problem that sounded like it could be proved with little trouble. A French mathematician wrote in the margin of a book nearly 400 years ago. He had a simple proof, he claimed, but no room to write it. He died without revealing what that proof was and he left mathematicians frustrated and tantalized.

Some of the greatest mathematicians of their time spent endless years trying to figure the problem out. There were false proofs along the way, and rewards. But the problem just resisted the best attempts to tackle it.

Then, in 1996, a Princeton mathematician, Andrew Wiles, came out of an attic room where he had worked alone for seven years and announced he had a proof. What followed was a nervous year of ups and downs. There was a hole in the proof. Could he fix it? Would

someone else fix it and share the glory? The *Times* stories tell the tale as it happened.

Less elegant, to mathematicians at least, was a proof of another old problem, the four-color conjecture. Like Fermat's Last Theorem, it was simple to state and seemed like it must be true: Can you color any map you might invent with just four colors so that no two adjacent regions have the same color? Mathematicians could prove that three colors were not enough and that five would work. But the question of whether four colors sufficed eluded them.

Finally, in 1976, two mathematicians proved it. But their proof was not the sort of elegant object of beauty that mathematicians crave. Instead, the mathematicians used a computer to do seemingly endless and onerous calculations, using—in those earlier days of computing—1,200 hours of computer time during which 10 billion logical decisions were made. Some mathematicians complained that the work was not elegant enough to count as a true proof, relying as it did on all those computer calculations. But no one has yet found a more elegant proof, and so it stands.

The most recent famous problem to fall was the Poincaré conjecture, a longstanding challenge that involved questions about three-dimensional space. Like Fermat's Last Theorem and the four-color conjecture, it was a conjecture that seemed like it had to be true, but no one could prove it until 2003, when an elusive Russian mathematician, Grigori Perelman, posted a few papers on the Internet making an extraordinary claim—he had solved the problem. His is a story of genius and self-imposed isolation. He refused a \$1 million prize, and he refused mathematics' highest honor, a Fields Medal, which is mathematics' version of a Nobel Prize.

Dennis Overbye writes in a Q and A on Perelman's work, "Everybody agrees that it is no surprise that the conjecture is true. What is surprising is the way it was proved, using mathematics far removed from traditional topology, establishing links no one had suspected between disparate fields and techniques. The same was true for Andrew Wiles's heroic proof of Fermat's Last Theorem in 1994."

New Mathematics Links Two Worlds

By WILLIAM L. LAURENCE

An important extension of modern mathematical methods, which promises to bridge the gap between the universe of the stars and the world of the atom, embracing at last the relativity and quantum theories, was presented here today before the Harvard tercentenary conference of the arts and sciences.

The new mathematics, which extends further the mathematics that made possible Einstein's theory of relativity, was presented here for the first time by Professor Élie Joseph Cartan, mathematician, of the University of Paris. His paper dealt with "the extension of tensor analysis to non-affine geometries," which unifies several modern mathematical developments into a new synthesis.

Another contribution, dealing with "truth in mathematics and logic," and offering a "new form of logic," was presented by Professor Rudolf Carnap, philosopher, formerly of the universities of Vienna and Prague, who will join the faculty of the University of Chicago next month.

These adventures in the highest realms of mind, mathematics and logic were described before a meeting held jointly with the American Mathematical Society, the Mathematical Association of America and the Association for Symbolic Logic.

The contributions were described as epoch-making by authorities present, who at the same time admitted that the material presented was of such a profound and abstruse nature that months of concentrated effort would be required to comprehend and digest it.

Hopes to Unify Two Systems

It was the development in recent times of the mathematical system known as "tensor analysis" that made it possible for Einstein to develop his theory of relativity. On the other hand, the theory of the new quantum mechanics, developed by (Paul) Dirac, (Werner) Heisenberg and others, was the outgrowth of an entirely different system of mathematics.

Professor Cartan has now extended the system of tensor analysis in such a way that for the first time it embraces systems of mathematics applicable to the quantum theory. Thus he hopes that at last a way has been opened for solving

one of the greatest problems in modern science, the unification of the two great systems of thought which alone make the physical universe understandable.

The search for a unified principle underlying his universe has been one of man's greatest intellectual cravings since the earliest days. From the Greek philosopher Thales down to the present it has been man's intuitive belief, amounting to a conviction, that the world he lives in, from the smallest atom to the totality of the stars and galaxies, is governed by a set of universal laws applicable throughout the entire realm.

There have been times in man's intellectual history when philosophers believed that they had achieved the goal in the search for the underlying, all-embracing principle governing all things. Then came modern science, with the extension of man's knowledge far out in space and deep within the atom, which shattered his dream of universal monism.

For he found, to his disappointment, that the set of mathematical laws by which he could gain an insight into the infinitesimal but infinite universe of the atom was totally different from the principles which embraced the totality of the new stars and galaxies.

Science has thus found itself faced with this vexing duality, a universe made up of atoms which has to have two sets of principles to explain it, one set (relativity) for the whole, and another set (quantum mechanics) for the building blocks (atoms) out of which the whole is constituted.

Discussion by Experts Awaited

Thus any extension of present mathematical systems that promises to supply the missing link between the two dual systems is regarded as of the highest importance to science.

(Albert) Einstein, (Arthur) Eddington, (Tullio) Levi-Civita and several others of the world's outstanding mathematical physicists are attending the tercentenary conference, and are expected to discuss the latest development in man's search for unity in consultations which might yield historic results. Dr. Cartan stated after the lecture that he expected to discuss the possibilities of his new mathematics with Einstein here.

Only the introduction to Dr. Cartan's paper is quotable for the general reader. He then plunged into such deep mathematical waters that even many experts present confessed they found it difficult to follow.

"It is unnecessary to recall the great services which tensor analysis has rendered to geometry and to mathematical physics," Dr. Cartan began. "Every one is aware that Einstein's general theory of relativity might not have been conceived had this admirable instrument of research not been created, under the name of 'absolute differential calculus,' by G. Ricci and T. Levi-Civita."

Difficulties of Adaptation Cited

"In its original form tensor analysis is marvelously adapted to Riemannian geometry and especially to the geometries with affine connections which have sprung up in the wake of the great movement created by the discovery of general relativity.

"This movement, it is true, did not stop at tensor analysis, and the geometries with projective, or conformal, connections, and others, have been added to Riemannian geometry, just as the classical projective, or conformal, geometries, and, in a general way, the different geometries of Klein, have been added to that of Euclid.

"But it is rather difficult to adapt tensor analysis to these generalized geometries, and the attempts to do so often give the impression of being artificial and of seeking principally to preserve the external form of the theory of Ricci and Levi-Civita in cases where it is contrary to the nature of the facts.

"I would like to show, in this lecture, the point of view which might be assumed in order to build up a general theory of tensor analysis; that is, a theory which would be applicable to the present state of differential geometry."

Later Dr. Cartan said: "The principal application, one could almost say the only one, which makes a generalization of the absolute differential calculus indispensable is related to the theory of generalized spaces, and particularly to the necessary and sufficient condition for applicability (of geometric identity of structure) of two spaces of the same nature."

Dr. Carnap States Problem

Professor Carnap first described the work of Dr. K. Gödel, Vienna mathematician, who showed that methods of modern mathematics were "incomplete." He then described his own method, which, he stated, would eliminate present difficulties in the logic of mathematics.

The first problem is to establish what is the nature of the truth of mathematical and logical theorems, Dr. Carnap stated. To do so, we must distinguish between what is known as factual truth and formal truth.

A statement of empirical science is true or false according to whether the possible fact asserted by it exists or not. A statement in the language of mathematics and logic does not assert a fact. Such a statement is true or false "according as the rules of the language system state it to be true; that is, capable of analysis, or false, namely, contradictory to the rules."

The second problem, Dr. Carnap said, is how to construct a system of mathematics, i.e., how to define the concept "true mathematical statement."

The customary method of demonstration, he said, consists of laying down some primitive postulates and some rules of inference, with a finite number of premises. For example, the system known as *principia mathematica*. According to the results of Dr. Gödel, however, such a system is always incomplete.

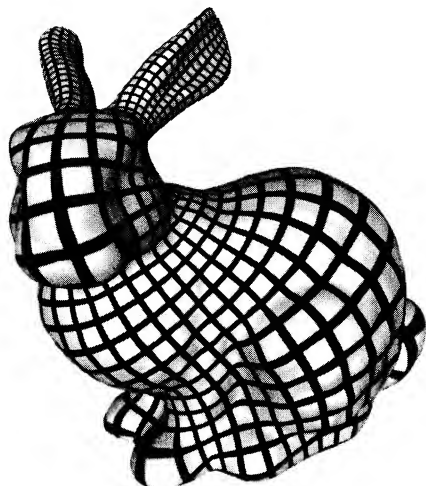
"Therefore, we are compelled," Dr. Carnap said, "to apply rules of a new kind, referring to infinite classes of premises. By rules of this kind the concept of the truth of universal statements concerning integers can easily be defined.

"However, for statements concerning real numbers, i.e., classes of integers, certain difficulties arise."

September 2, 1936

An Elusive Proof and Its Elusive Prover

By DENNIS OVERBYE



Grisha Perelman, where are you?

Three years ago, a Russian mathematician by the name of Grigori Perelman, aka Grisha, in St. Petersburg, announced that he had solved a famous and intractable mathematical problem, known as the Poincaré conjecture, about the nature of space.

After posting a few short papers on the Internet

and making a whirlwind lecture tour of the United States, Dr. Perelman disappeared back into the Russian woods in the spring of 2003, leaving the world's mathematicians to pick up the pieces and decide if he was right.

Now they say they have finished his work, and the evidence is circulating among scholars in the form of three book-length papers with about 1,000 pages of dense mathematics and prose between them.

As a result there is a growing feeling, a cautious optimism that they have finally achieved a landmark not just of mathematics, but of human thought.

"It's really a great moment in mathematics," said Bruce Kleiner of Yale, who has spent the last three years helping to explicate Dr. Perelman's work. "It could have happened 100 years from now, or never."

In a speech at a conference in Beijing this summer, Shing-Tung Yau of Harvard said the understanding of three-dimensional space brought about by Poincaré's conjecture could be one of the major pillars of math in the 21st century.

Quoting Poincaré himself, Dr. Yau said, "Thought is only a flash in the middle of a long night, but the flash that means everything."

But at the moment of his putative triumph, Dr. Perelman is nowhere in sight. He is an odds-on favorite to win a Fields Medal, math's version of the Nobel Prize,

when the International Mathematics Union convenes in Madrid next Tuesday. But there is no indication whether he will show up.

Also left hanging, for now, is \$1 million offered by the Clay Mathematics Institute in Cambridge, Mass., for the first published proof of the conjecture, one of seven outstanding questions for which they offered a ransom back at the beginning of the millennium.

"It's very unusual in math that somebody announces a result this big and leaves it hanging," said John Morgan of Columbia, one of the scholars who has also been filling in the details of Dr. Perelman's work.

Mathematicians have been waiting for this result for more than 100 years, ever since the French polymath Henri Poincaré posed the problem in 1904. And they acknowledge that it may be another 100 years before its full implications for math and physics are understood. For now, they say, it is just beautiful, like art or a challenging new opera.

Dr. Morgan said the excitement came not from the final proof of the conjecture, which everybody felt was true, but the method, "finding deep connections between what were unrelated fields of mathematics."

William Thurston of Cornell, the author of a deeper conjecture that includes Poincaré's and that is now apparently proved, said, "Math is really about the human mind, about how people can think effectively, and why curiosity is quite a good guide," explaining that curiosity is tied in some way with intuition.

"You don't see what you're seeing until you see it," Dr. Thurston said, "but when you do see it, it lets you see many other things."

Depending on who is talking, Poincaré's conjecture can sound either daunting or deceptively simple. It asserts that if any loop in a certain kind of three-dimensional space can be shrunk to a point without ripping or tearing either the loop or the space, the space is equivalent to a sphere.

The conjecture is fundamental to topology, the branch of math that deals with shapes, sometimes described as geometry without the details. To a topologist, a sphere, a cigar and a rabbit's head are all the same because they can be deformed into one another. Likewise, a coffee mug and a doughnut are also the same because each has one hole, but they are not equivalent to a sphere.

In effect, what Poincaré suggested was that anything without holes has to be a sphere. The one qualification was that this "anything" had to be what mathematicians call compact, or closed, meaning that it has a finite extent: no matter how far you strike out in one direction or another, you can get only so far away before

you start coming back, the way you can never get more than 12,500 miles from home on Earth.

In the case of two dimensions, like the surface of a sphere or a doughnut, it is easy to see what Poincaré was talking about: imagine a rubber band stretched around an apple or a doughnut; on the apple, the rubber band can be shrunk without limit, but on the doughnut it is stopped by the hole.

With three dimensions, it is harder to discern the overall shape of something; we cannot see where the holes might be. "We can't draw pictures of 3-D spaces," Dr. Morgan said, explaining that when we envision the surface of a sphere or an apple, we are really seeing a two-dimensional object embedded in three dimensions. Indeed, astronomers are still arguing about the overall shape of the universe, wondering if its topology resembles a sphere, a bagel or something even more complicated.

Poincaré's conjecture was subsequently generalized to any number of dimensions, but in fact the three-dimensional version has turned out to be the most difficult of all cases to prove. In 1960 Stephen Smale, now at the Toyota Technological Institute at Chicago, proved that it is true in five or more dimensions and was awarded a Fields Medal. In 1983, Michael Freedman, now at Microsoft, proved that it is true in four dimensions and also won a Fields.

"You get a Fields Medal for just getting close to this conjecture," Dr. Morgan said.

In the late 1970s, Dr. Thurston extended Poincaré's conjecture, showing that it was only a special case of a more powerful and general conjecture about three-dimensional geometry, namely that any space can be decomposed into a few basic shapes.

Mathematicians had known since the time of Georg Friedrich Bernhard Riemann, in the 19th century, that in two dimensions there are only three possible shapes: flat like a sheet of paper, closed like a sphere, or curved uniformly in two opposite directions like a saddle or the flare of a trumpet. Dr. Thurston suggested that eight different shapes could be used to make up any three-dimensional space.

"Thurston's conjecture almost leads to a list," Dr. Morgan said. "If it is true," he added, "Poincaré's conjecture falls out immediately." Dr. Thurston won a Fields in 1982.

Topologists have developed an elaborate set of tools to study and dissect shapes, including imaginary cutting and pasting, which they refer to as "surgery," but they were not getting anywhere for a long time.

In the early 1980s Richard Hamilton of Columbia suggested a new technique, called the Ricci flow, borrowed from the kind of mathematics that underlies Einstein's general theory of relativity and string theory, to investigate the shapes of spaces.

Dr. Hamilton's technique makes use of the fact that for any kind of geometric space there is a formula called the metric, which determines the distance between any pair of nearby points. Applied mathematically to this metric, the Ricci flow acts like heat, flowing through the space in question, smoothing and straightening all its bumps and curves to reveal its essential shape, the way a hair dryer shrinks wraps plastic.

Dr. Hamilton succeeded in showing that certain generally round objects, like a head, would evolve into spheres under this process, but the fates of more complicated objects were problematic. As the Ricci flow progressed, kinks and neck pinches, places of infinite density known as singularities, could appear, pinch off and even shrink away. Topologists could cut them away, but there was no guarantee that new ones would not keep popping up forever.

"All sorts of things can potentially happen in the Ricci flow," said Robert Greene, a mathematician at the University of California at Los Angeles. Nobody knew what to do with these things, so the result was a logjam.

It was Dr. Perelman who broke the logjam. He was able to show that the singularities were all friendly. They turned into spheres or tubes. Moreover, they did it in a finite time once the Ricci flow started. That meant topologists could, in their fashion, cut them off, and allow the Ricci process to continue to its end, revealing the topologically spherical essence of the space in question, and thus proving the conjectures of both Poincaré and Thurston.

Dr. Perelman's first paper, promising "a sketch of an eclectic proof," came as a bolt from the blue when it was posted on the Internet in November 2002. "Nobody knew he was working on the Poincaré conjecture," said Michael T. Anderson of the State University of New York in Stony Brook.

Dr. Perelman had already established himself as a master of differential geometry, the study of curves and surfaces, which is essential to, among other things, relativity and string theory. Born in St. Petersburg in 1966, he distinguished himself as a high school student by winning a gold medal with a perfect score in the International Mathematical Olympiad in 1982. After getting a Ph.D. from St. Petersburg State, he joined the Steklov Institute of Mathematics at St. Petersburg.

In a series of postdoctoral fellowships in the United States in the early 1990s, Dr. Perelman impressed his colleagues as “a kind of unworldly person,” in the words of Dr. Greene of U.C.L.A.—friendly, but shy and not interested in material wealth.

“He looked like Rasputin, with long hair and fingernails,” Dr. Greene said.

Asked about Dr. Perelman’s pleasures, Dr. Anderson said that he talked a lot about hiking in the woods near St. Petersburg looking for mushrooms.

Dr. Perelman returned to those woods, and the Steklov Institute, in 1995, spurning offers from Stanford and Princeton, among others. In 1996 he added to his legend by turning down a prize for young mathematicians from the European Mathematics Society.

Until his papers on Poincaré started appearing, some friends thought Dr. Perelman had left mathematics. Although they were so technical and abbreviated that few mathematicians could read them, they quickly attracted interest among experts. In the spring of 2003, Dr. Perelman came back to the United States to give a series of lectures at Stony Brook and the Massachusetts Institute of Technology, and also spoke at Columbia, New York University and Princeton.

But once he was back in St. Petersburg, he did not respond to further invitations. The e-mail gradually ceased.

“He came once, he explained things, and that was it,” Dr. Anderson said. “Anything else was superfluous.”

Recently, Dr. Perelman is said to have resigned from Steklov. E-mail messages addressed to him and to the Steklov Institute went unanswered.

In his absence, others have taken the lead in trying to verify and disseminate his work. Dr. Kleiner of Yale and John Lott of the University of Michigan have assembled a monograph annotating and explicating Dr. Perelman’s proof of the two conjectures.

Dr. Morgan of Columbia and Gang Tian of Princeton have followed Dr. Perelman’s prescription to produce a more detailed 473-page step-by-step proof only of Poincaré’s conjecture. “Perelman did all the work,” Dr. Morgan said. “This is just explaining it.”

Both works were supported by the Clay Institute, which has posted them on its Web site, claymath.org. Meanwhile, Huai-Dong Cao of Lehigh University and Xi-Ping Zhu of Zhongshan University in Guangzhou, China, have published their own 318-page proof of both conjectures in *The Asian Journal of Mathematics* (www.ims.cuhk.edu.hk/).

Although these works were all hammered out in the midst of discussion and argument by experts, in workshops and lectures, they are about to receive even stricter scrutiny and perhaps crossfire. "Caution is appropriate," said Dr. Kleiner, because the Poincaré conjecture is not just famous, but important.

James Carlson, president of the Clay Institute, said the appearance of these papers had started the clock ticking on a two-year waiting period mandated by the rules of the Clay Millennium Prize. After two years, he said, a committee will be appointed to recommend a winner or winners if it decides the proof has stood the test of time.

"There is nothing in the rules to prevent Perelman from receiving all or part of the prize," Dr. Carlson said, saying that Dr. Perelman and Dr. Hamilton had obviously made the main contributions to the proof.

In a lecture at M.I.T. in 2003, Dr. Perelman described himself "in a way" as Dr. Hamilton's disciple, although they had never worked together. Dr. Hamilton, who got his Ph.D. from Princeton in 1966, is too old to win the Fields Medal, which is given only up to the age of 40, but he is slated to give the major address about the Poincaré conjecture in Madrid next week. He did not respond to requests for an interview.

Allowing that Dr. Perelman, should he win the Clay Prize, might refuse the honor, Dr. Carlson said the institute could decide instead to use award money to support Russian mathematicians, the Steklov Institute or even the Math Olympiad.

Dr. Anderson said that to some extent the new round of papers already represented a kind of peer review of Dr. Perelman's work. "All these together make the case pretty clear," he said. "The community accepts the validity of his work. It's commendable that the community has gotten together."

August 15, 2006

Ask Science: Poincaré's Conjecture

By DENNIS OVERBYE

Dennis Overbye answered select reader questions regarding his article about the Poincaré conjecture from this week's *Science Times*.

Q. The Poincaré conjecture article has a side note stating, "To a topologist, a rabbit is the same as a sphere." Every rabbit I've seen, however, has a hole (or tunnel if you prefer) running from its mouth to just under its tail. It seems to me a rabbit is really the same as a donut. —*F. P. Katz*

A. So you see, topology isn't so hard after all. More readers than I care to count—by far a vast majority of those of you who wrote and phoned through all the different channels of communication available—took issue with my oversimplification of rabbit anatomy. Some were more scatological than the others. Yes, real live rabbits are like doughnuts, as are people, worms and sharks. As more than one reader pointed out, the development of a digestive system is no small feat for an organism.

My only excuse, and I admit it is a feeble one, is that the bunny in the graphic that accompanied this story was clearly a cleaned up version with no orifices, more like a chocolate bunny or a Disney animal than a real one. I also have to say that I never owned a rabbit, or any animal that lived in a cage that had to be cleaned up—an experience that might have reminded me of the inconvenient side of bunnies.

A mathematician friend tells me that the fact that so many readers caught me on this is very encouraging. "You should be ecstatic over this," he wrote in an e-mail. "It means that a lot of non-mathematicians actually understood what you wrote!"

Q. Not surprisingly, I'm having difficulty imagining the eight fundamental shapes of three-dimensional space. Can you help me visualize these? —*C. Horwitz*

A. If I could visualize the fundamental shapes of three-dimensional space, I would have leaned on the art department to put them in the paper, but this is

where the imagination goes “sproinggg!” There is a list of the eight geometries on Thurston’s geometrization conjecture at <http://mathworld.wolfram.com/ThurstonsGeometrizationConjecture.html>, among other places. But buyer beware. Not all these geometries are yet well understood, and so yes, there is work to be done. Whether it will take another century, nobody knows.

Q. To what extent does the new proof of the Poincaré conjecture have implications for physics, given the connection between Ricci flows and string theory? —*A. Morgan*

Q. The article refers to the Poincaré conjecture as not only famous but important. In what way(s) is proof of the conjecture important and what may be the practical implications, if any? Thank You! —*J. Vita, New Haven, Connecticut*

Q. Thank you for an interesting article, but I still don’t understand the importance of Poincaré’s conjecture or the implications of the proof. For example, will this new finding further space travel? Does it have application to economics? Or is it only of interest to mathematics in the way that a challenging chess problem is only of interest to other chess players? —*A. Driesbach*

A. Everybody agrees that it is no surprise that the conjecture is true. What is surprising is the way it was proved, using mathematics far removed from traditional topology, establishing links no one had suspected between disparate fields and techniques. The same was true for Andrew Wiles’s heroic proof of Fermat’s Last Theorem in 1994.

That this will eventually redound to the glory physics is beyond doubt. The problem is that the mathematicians are generally a century ahead of the physicists. So nobody can forecast where this new math will prove decisive.

When I asked Edward Witten, a physicist at the Institute for Advanced Study and also a Fields medalist as a mathematician, he pointed out the two-dimensional version of Poincaré’s conjecture was done in the middle of the 19th century, by the visionary German mathematician Georg Friedrich Bernhard Riemann, when he classified surfaces. Now it is very important in general relativity and in string theory.

“But no one foresaw how that would happen 100 years ago when the original mathematical work was done,” Dr. Witten wrote in an e-mail the other week, “So it is going to be hard for me to guess what role the Poincaré problem might ultimately prove to play.”

Q. You describe the Ricci flow as a “technique.” Is it an equation? How exactly is it “applied mathematically” to the metric (which is also an equation, yes?)? —*E. Rose*

A. Technically, the Ricci flow is a differential equation. When you solve it, the metric has been deformed and becomes smoother over time.

Q. When you say, “Likewise, a coffee mug and a doughnut are also the same because each has one hole, but they are not equivalent to a sphere,” shouldn’t you have added that the mug must have a conventional handle to be topologically equivalent to a donut?

It seems to me that a mug without a handle can be deformed into a sphere (picture inflating the seamless but folded surface of the handleless mug). Then, the addition of the handle is equivalent to a handle on a sphere and, of course, that’s equivalent to a donut with an aneurysm, which is equivalent to a donut.

This, of course, is not formal mathematics; I’m just running animations in my imagination, which behavior is what interested me in math in the first place in 1962 when I was in tenth grade. I went on to get a mathematics BA but, ironically, never went anywhere with the degree having been repelled by, you guessed it, topology (or, rather, a haughty, dismissive topology professor in my senior year). —*J. Broido*

A. Yes, you need a handle on the mug for it to be transformable into a sphere. Your topology professor dismissed you too soon.

Q. Your example of a rubber band stretched around an apple or a doughnut is unclear—at least to a scientific ignoramus like me. When I picture a band stretched around an apple shrinking, the band starts to cut into the apple and bisect it. I don’t know what you mean when you say the band can be “shrunk without limit,” or when you say that the band will

be "stopped" by a doughnut hole. Can you illustrate this some other way?
—*R. Rodriguez*

A. You could imagine a little lasso lying on the surface of whatever. Then if you can tighten the lasso all the way so that the loop disappears into the knot, then the surface doesn't have a hole in it and might be a sphere, topologically. If there is a hole, though, the lasso might go around it, like the long way around a doughnut; then you can't tighten it to be smaller than the hole in the doughnut and still keep it on the surface.

Q. I read this article with some interest in the Poincaré conjecture, about the nature of space. As I think about this, and obviously I do not have the tools of any of these mathematicians and I have the fear of being thought crazy even to think I really understand this proof let alone the implications. Still, I wonder if this mathematical proof is saying in effect that space of more than three dimensions must be "spherical" means that a worm hole tunneling between two points in our universe cannot exist because the shape that space-time must assume can not exist. Darn it sounds crazy. In addition, space-time cannot be torn because the shape it would need to form can not exist.

Help. If I am on the wrong track and off base for trying to understand the physics through the math please humor me with some response. —*M. Novak*

A. You raise a challenging question. There's a lot we don't know yet about the topology of the four-dimensional space-time in which we live. That is to say, we don't know if all the loops can close down to zero. Wormholes would catch them up. I don't think anyone has proved that real space-time is "spherical" yet.

Q. Before you go on reporting on the conjecture, you should certainly read A. Garciadiego's *Bertrand Russell and the Origins of the Set-Theoretic "Paradoxes."* It's horribly proofread, but it's a landmark in the history of mathematics (published in 1992).

Remember that Poincaré's project was to avoid the paradoxes he felt had been generated by set theory. Garciadiego's book shows that the supposed

paradoxes were not paradoxes at all. This immediately brings into question the goal of the conjecture. I think you will find that there are assumptions about the nature of a set, built into the conjecture, which are highly questionable. Certainly you will find Cantor's set notions highly questionable after you read Garciadiego.

In the end, I think there is considerable doubt growing that Poincaré's conjecture IS a conjecture. This is something which has not been considered by the mathematicians you name. —*J. Ryskamp*

A. I'm not aware of Garciadiego's work. Thanks for bringing it to my attention.

Q. You are to be commended for your article on recent developments in the proof of the Poincaré conjecture (NYT Science, 15 August). You have made a very difficult concept somewhat accessible to many of us who are not mathematicians.

Topology has been central to the field of chemistry for as long as we know. Since ancient Greek description of materials (atoms as spheres with hooks on them), those of us interested in the properties of matter have found it necessary to rely on an abstract symbolic representation of the size and shapes of atoms and molecules in order to effectively understand and describe the properties that we observe. Our views today are slightly more sophisticated than those of the Greeks. Molecular structures are represented by connected partial spheres representing the constituent atoms, and lead to shapes of molecules. Reasonably impenetrable surface electron clouds provide the shapes of molecules as we have come to perceive them. Together with differences in electron density, these shapes provide the foundation to our description of how molecular structures interact with each other. This understanding is central to modern chemical reaction studies, and is essential to the rapidly developing field of molecular biology and genetics.

You point out in your article that the Poincaré conjecture is fundamental to topology. In your interviews and research while preparing the article, did you encounter any topologists who have begun to speculate about the possibility that current work that might lead to an improvement in our understanding of the geometry, shapes and interaction of molecular structures?

You can appreciate that a significantly improved understanding of the topology of molecules could provide profound improvement in our understanding of chemical reactions. You note that some of your sources speculate that "it may be another 100 years before its full implication for math and physics are understood." We can hope that it is not that long before it exerts an effect on our understanding of chemical reactivity.

I would be interested in learning if your preparation of this article provided you any information on researchers who are actively pursuing this point. —*J. Casanova*

A. A quick Google search yielded many results relating to topology and chemistry, though none of the people I talked to are involved. Dr. Yau and his colleagues have applied some of these techniques to analyzing images of brains from M.R.I. machines.

A more speculative development is the prospect of topological computers, a concept being investigated by Michael Freedman of Microsoft, who won a Fields Medal for proving the Poincaré conjecture in four dimensions, and Caltech's Alexei Kitaev. The idea is that knots or loops in a fluid of cold electrons could form the basis of a quantum computer.

August 18, 2006

Grigori Perelman's Beautiful Mind

By JASCHA HOFFMAN

In 1904 the French mathematician Henri Poincaré made a conjecture about three-dimensional space that may help to explain the shape of the universe. Although it was crucial to the growth of the field of topology, Poincaré's conjecture resisted proof for a century. When a Boston philanthropist announced a million-dollar prize for its solution in 2000 it was unclear whether he would ever have to pay.

Then, in 2002, a Russian mathematician named Grigori Perelman posted a terse paper to an online archive. In the course of tackling a broader problem, Perelman seemed to have miraculously swept away the remaining obstacles to proving the Poincaré conjecture. Soon the mathematical rumor mill was buzzing. The proof seemed genuine, but word was that Perelman had no plans to publish it.

This was only the beginning of the weirdness. After a brief trip to the United States with his mother in tow, Perelman retreated to St. Petersburg and ceased communication with all but a few colleagues vetting his work. He declined the Fields Medal, a gesture equivalent to snubbing the Nobel committee. He then resigned from the Steklov Institute in 2005 with a letter that read, "I have been disappointed in mathematics and I want to try something else."

Why did Perelman turn his back on the world? This question haunts Masha Gessen's *Perfect Rigor*, a dogged portrait of an elusive man. Gessen, a Russian-born journalist who has written books on the post-Soviet intelligentsia and on the pitfalls of genetic testing, is no stranger to the burdens of uncommon knowledge. Without a shred of help from Perelman himself, she charts the mathematician's rise from quiet super-student to prickly genius, suggesting that the very perfectionism that fueled his work may have been the cause of his alienation.

Born to a mother whose own math career was foiled by discrimination, the young Perelman excelled at the distinctly Russian sport of competitive mathematics in the 1970s. Gessen gives ample background on his coaches and classmates, who describe him mostly as "a sort of math angel" who never made mistakes. Stuck with a tricky problem, the young Perelman would bounce a Ping-Pong ball against his desk, vigorously rub his thigh and hum or moan until he had the answer.

By the time Perelman got to university, his fingernails were so long they had begun to curl. He wanted little more than to continue his work undisturbed—and protected by a Who's Who of Russian mathematicians, he seems to have gotten his wish. After emerging from graduate school as the Soviet Union crumbled, Perelman taught briefly in the United States in the early 1990s (where he wore the same brown corduroy jacket day after day and survived on a diet of black bread and fermented milk). But soon he returned to St. Petersburg and the seclusion of his mother's apartment. It was there that he would spend most of a decade working on the Poincaré conjecture.

Perhaps because of his silence, Perelman has become a kind of mathematical Rorschach test. Some of his peers see him as a righteous nonconformist, others as a cranky purist. Drawing on interviews with colleagues scattered from France to Israel, Gessen proposes that Perelman's disillusionment was a product of the same "rigid, demanding and hypercritical" habits of mind that made him a genius. With an armchair diagnosis of Asperger's syndrome, she suggests that he was unable, and not simply unwilling, to play by anyone's rules but his own.

Given the lack of firsthand evidence about Perelman's motives, one could have hoped for a clearer sense of the work he pursued with such devotion. Gessen, herself a "math junkie" in school, confines the math to a single difficult chapter. (Readers who want more should consult Donal O'Shea's lucid book, *The Poincaré Conjecture*.) But she does provide a thorough account of the circumstances that led to Perelman's rise in the "vicious, backstabbing little world" of Soviet mathematics and a brilliant reconstruction of the twisted logic that might have led to his mysterious exit. In so doing she has written something rare: an accessible book about an unreachable man.

December 10, 2009

A Math Problem Solver Declines a \$1 Million Prize

By DENNIS OVERBYE

The reclusive Russian mathematician Grigori Perelman, aka Grisha, gained worldwide fame by claiming to have solved one of the world's most intractable mathematical problems, the Poincaré conjecture, and then disappearing in St. Petersburg. On Thursday he said he had rejected a \$1 million prize from the Clay Mathematics Institute in Cambridge, Mass., for the feat.

"I have refused," Interfax, a Russian news agency, quoted him as saying. "You know, I had quite a lot of reasons both for and against. That is why I took so long to make up my mind."

James Carlson, president of the Clay Institute, said he had spoken with Dr. Perelman by phone. "He was, as usual, quite pleasant, though quite firm in his decision," Dr. Carlson said.

The problem, named after the great French polymath Henri Poincaré, has led mathematicians on a frustrating chase for a century. It hypothesizes that any three-dimensional space without holes is essentially a sphere.

In 2003, Dr. Perelman posted a series of papers on the Internet claiming to have proved the conjecture, and a deeper problem by the Cornell mathematician William Thurston, building on work by Richard Hamilton, a Columbia University mathematician.

After a brief barnstorming tour in the United States, during which he refused interviews, Dr. Perelman returned to Russia, leaving the world's mathematicians to pick up the pieces and decide whether he had really done it.

A worldwide race to retrace, explicate and check Dr. Perelman's proof ensued. In the meantime, Dr. Perelman quit his post at the Steklov Mathematical Institute, moved in with his mother and ceased communicating with the outside world.

By 2006, as learned papers totaling more than a thousand pages of dense mathematics slouched toward publication, it was becoming apparent that Dr. Perelman had indeed solved the conjecture, and he was awarded a Fields Medal, the most prestigious award in mathematics, at the International Congress of Mathematicians in Madrid.

Dr. Perelman, who already had a history of declining awards, did not show.

So when the Clay Institute announced in March that he had won the big prize, many doubted that he would accept. In June, a three-day symposium in Paris celebrating the proof of the conjecture went on without him.

Dr. Perelman said Dr. Hamilton deserved as much credit as he did, Interfax reported. "To put it short," he said, "the main reason is my disagreement with the organized mathematical community. I don't like their decisions; I consider them unjust."

The Clay Institute said it would announce this fall how it would spend the award money.

July 1, 2010

"Four-Color Problem" Attacked

By WILLIAM L. LAURENCE

A new mathematical generalization which offers an indirect methods for solving what is known as "the four-color problem," namely, how to make a map embracing any number of regions without using more than four colors, in such a manner that the same color is not used for adjoining areas, was presented by Professor George D. Birkhoff, dean of the graduate faculty and professor of mathematics at Harvard University.

"It is almost certain that every map can be colored in only four colors," said Professor Birkhoff, "but mathematics, despite arduous efforts, have not been able to establish that four colors suffice in every case, although it is easily proved that five colors are sufficient." The latest result, due to Professor Philip Franklin of the Massachusetts Institute of Technology, shows that four colors only are required for maps of not more than 31 regions. This represents the high water mark of the results so far obtained."

Professor Birkhoff described a generalized mathematical equation in which the four-color problem could be fitted in as part of a larger whole. The method may be compared to the magnification of a minute object by means of a microscope in order to bring it within the field of visibility.

April 21, 1939

Four-Color Proof

Mathematics is central to every aspect of modern civilization—from space navigation to the formulation of business strategy in the corporate world. Yet so highly abstract is the nature of most modern mathematical research that only on rare occasions is some major advance achieved whose nature is comprehensible to non-mathematicians.

An example is the recently successful proof of the four-color conjecture, one of the classic problems that has engaged mathematicians of many nations during the past two centuries. It can be stated simply: Given a map of any kind, perhaps of the countries of the world, or the states of a nation, or of all America's countries, etc., what is the minimum number of colors required so that no two adjacent regions—countries, states, counties, or whatever—are shown in the same color? Almost a century ago it was proved that five colors would suffice, but the conjecture that four colors would be enough has baffled generation after generation of the world's most talented mathematicians.

Now the four-color conjecture has been proved by two University of Illinois mathematicians, Kenneth Appel and Wolfgang Haken. They had an invaluable tool that earlier mathematicians lacked—modern computers. Their present proof rests in part on 1,200 hours of computer calculation during which about ten billion logical decisions had to be made.

The proof of the four-color conjecture is unlikely to be of applied significance. Nevertheless, what has been accomplished is a major intellectual feat. It gives us an important new insight into the nature of two-dimensional space and of the ways in which such space can be broken into discrete portions.

September 24, 1976

Goldbach's Conjecture; This One May Be Provable, but We May Never Know

By GEORGE JOHNSON

When a Russian civil servant named Christian Goldbach sent a letter to the Swiss mathematician Leonhard Euler in 1742, seeking advice about a maddeningly recalcitrant problem, he could hardly have imagined that more than two centuries later it would remain unsolved.

He would certainly have been astonished to know that Alan Turing, whose story recently came to Broadway in the play *Breaking the Code*, would show in 1937 that a solution to Goldbach's Conjecture, as it came to be called, might never be found.

Goldbach, who had served as tutor to Peter II, the teenaged czar, surmised that every even number can be represented as the sum of two primes. Primes, the atoms of mathematics, are numbers such as 2, 3, 5, 7 and 11 that have no divisors other than themselves and 1.

Following Goldbach, the number 10, for example, can be written as the sum of 3 and 7, and 24 as the sum of 17 and 7. Try as he might, Goldbach could not find an even number that could not be expressed this way. Using computers, mathematicians have tested every even number up to at least 100 million and have found no exceptions. But there is still no guarantee that the next number they examine won't violate the rule.

A tiny bit of progress in proving that Goldbach's Conjecture always holds true was made in 1930, when it was demonstrated that no matter how large a number is, it will never take more than 800,000 primes, added together, to represent it. This was a far cry from proving that all even numbers are the sum of two primes, but mathematicians considered it a helpful start. In 1941, Ivan Matveyevich Vinogradov came closer to the mark and received a 100,000-ruble prize from Stalin.

During most of the quest, mathematicians assumed that, just as monkeys banging on typewriters would eventually produce a line of Shakespeare, so would Goldbach's Conjecture be solved. Then in 1931, to universal dismay, the German mathematician Kurt Gödel showed that there will always be problems that are, in principle, unsolvable. Goldbach's Conjecture might be among them.

But how could we ever tell? It is a simple matter to write a computer program to test numbers, one after the other, stopping if it finds a violation of the rule. Now, if only it were possible to somehow analyze the program and prove that it eventually would halt, then we would know Goldbach was wrong. We wouldn't know which number was the culprit but at least it would be clear that one existed. Or, if we could show that the program would run interminably, we would have proved Goldbach's Conjecture.

Turing, alas, showed that it is impossible to know in advance whether this program—or any other—will eventually halt. The only way to find out is to wait, possibly forever.

If Goldbach's Conjecture is someday proved, it won't mean that Gödel or Turing was wrong. Other undecidable theorems undoubtedly exist. We just haven't stumbled across them.

April 17, 1988

Mathematics Expert May Soon Resolve a 350-Year Problem

By JAMES GLEICK

One of the most notorious unsolved problems of mathematics, a 350-year-old conjecture known as Fermat's Last Theorem, may be close to succumbing to a new line of attack, mathematicians said yesterday.

A Japanese number theorist, Yoichi Miyaoka, outlined a possible proof late last month at the Max-Planck Institute in Bonn. Notes of his presentation, jotted down by a colleague, have been circulating worldwide amid growing excitement.

Mathematicians said it was too early to know how to evaluate the new approach. Dr. Miyaoka has not even completed a manuscript.

If a detailed proof emerges, it will have to stand up to the scrutiny of scores of number theorists who are now waiting to see it.

Some Haunting Words

The 17th-century French mathematician Pierre de Fermat put forward the conjecture that now bears his name in about 1637, scribbling it in the margin of a Latin mathematics text. He asserted that no combination of whole numbers, zeroes aside, could satisfy the equation $x^n + y^n = z^n$ for n greater than 2.

When n equals 2, there are infinitely many solutions: pairs of perfect squares whose sum equals a third perfect square, such as $3^2 + 4^2 = 5^2$. Fermat's contention was that for cubes and higher powers, no such sum would ever be found.

He then added one of the most famous remarks in the annals of mathematics: "I have discovered a truly remarkable proof of this theorem which this margin is too small to contain." Those words have haunted his successors for centuries.

"The Lost Gold Mine"

"People have looked for El Dorado, the lost gold mine," said Ronald L. Graham, head of mathematical research at the American Telephone and Telegraph Company's Bell Laboratories. "People have tried to imagine what Fermat had in mind, given that he really didn't know so much."

Dr. Miyaoka's attack on the problem, which he hopes to complete within days, will be somewhat bulkier than Fermat's mysterious version, but still surprisingly succinct—perhaps just 5 to 10 pages, according to those familiar with it. So far, though, mathematicians remain cautious.

"Nobody has the right to have an opinion yet," said one number theorist. "The notes are very sketchy, and one probably shouldn't be able to conclude one way or the other."

March 10, 1988

Fermat's Theorem Solved? Not This Time

By JAMES GLEICK

The most notorious unsolved problem of mathematics, Fermat's Last Theorem, appears to have defeated yet another attack, put forward this month by a Japanese number theorist.

Experts who examined a draft manuscript by the number theorist Yoichi Miyaoka at the Max Planck Institute in Bonn, have found gaps that seem serious, at least for now.

"It's looking rather poor," said Don Zagier, another number theorist at the institute. "There have been many objections, some easily handleable, but now several points have arisen which at the very least are quite worrying. Miyaoka himself is now not sure that his proof is correct."

Amateurs and professionals alike have struggled for 350 years with this deceptively simple conjecture about numbers, scribbled in the margin of a Latin mathematics text by the great 17th-century mathematician Pierre de Fermat. He asserted that no combination of whole numbers, zeroes aside, could satisfy the equation $x^n + y^n = z^n$ for n greater than 2.

When n equals 2, there are infinitely many solutions: pairs of perfect squares whose sum equals a third perfect square, such as $3^2 + 4^2 = 5^2$. Fermat's contention was that for cubes and higher powers, no such sum would ever be found.

Dr. Miyaoka, who has been unwilling to comment publicly, tentatively proposed that he had proved a far more general result that, as a secondary by-product, would have proved Fermat's Last Theorem as well—or almost proved it. One loophole would have remained, which mathematicians said might have been closed with some computer calculations.

The history of mathematics is littered with failed proofs of Fermat's Last Theorem, but, to many mathematicians, the problem is beginning to seem less unreachable than in the past. Dr. Miyaoka, a distinguished mathematician who has made important advances in number theory, is working to salvage his approach.

"It's not quite that he's retracted the proof or that all is lost," Dr. Zagier said. "But there's still work to be done, and it may be a lot of work."

March 29, 1988

Fermat's Last Theorem Still Has 0 Solutions

By JAMES GLEICK

Not many of the old problems are left, and none is as notorious as Fermat's Last Theorem, so the telephone lines and computer message networks of the mathematics world buzzed over the last month with the news that this 350-year-old enigma of number theory might finally have succumbed.

It was just another false alarm. Colleagues of a Japanese mathematician, Yoichi Miyaoka, spread the word that a solution might be near, but when experts saw a preliminary manuscript, they quickly found what they politely describe as "gaps," or "places which deserve further elaboration." For now, at least, that makes Dr. Miyaoka just another victim—joining the hundreds of professionals and thousands of amateurs defeated over the centuries.

In a way, the few remaining historic puzzles have become anachronisms in modern mathematics, treasured more for their mystique than for their real importance. Dr. Miyaoka's approach actually addressed a far broader issue in the theory of numbers; had it solved Fermat's Last Theorem, it would have done so in passing, as a "by-product of a by-product of a by-product," as one mathematician put it.

"It's just one special thing," said another, Gerd Faltings of Princeton University. "Usually with mathematicians, when you solve something, you hope that the proof will allow you to do something else."

Still, the great old problems have an extraordinary power to enthrall.

As mathematics grows ever more abstruse and arcane, these rare problems are tantalizingly easy to state.

And in the universe of unsolved problems, Pierre de Fermat's—jotted around 1631 in the margin of a Latin text—has a special status. It has produced a mythology like no other question in pure mathematics, and for three centuries it has stood as a quirky island of human ignorance, while number theory grew up around it. "It's a reminder of how far we have to go as intelligent creatures," said Ronald Graham, head of mathematical research at A.T.&T.'s Bell Laboratories. "Not that we need constant reminders of that—but it's one more."

The essence of the theorem is so easy to grasp that amateurs have tackled it by the thousands, churning out false proofs that have clogged the mailboxes of university mathematics departments. Martin Gardner, the dean of recreational

mathematics and longtime “Mathematical Games” columnist of *Scientific American*, had postcards printed to decline requests from readers asking him to evaluate their versions.

A Marginal Proof

The theorem—more precisely, a conjecture—belongs to the theory of whole numbers. Fermat asserted that no solutions exist for the equation $a^n + b^n = c^n$ for n greater than 2. (Trivial solutions, containing zeroes, do not count.) When n equals 2, there are infinitely many solutions: pairs of perfect squares whose sum equals a third perfect square, such as $3^2 + 4^2 = 5^2$, or $5^2 + 12^2 = 13^2$. Fermat’s contention was that, for cubes and higher powers, no such sum would ever be found.

As famous as the problem itself is the pregnant comment that Fermat scribbled with it: “I have discovered a truly remarkable proof of this theorem which this margin is too small to contain.” That comment has echoed for centuries, an irritating goad to mathematicians. A few summers ago, a graffito appeared on a wall of New York City’s Eighth Street BMT subway station: Fermat’s equation and the words, “I have discovered a truly remarkable proof of this, but I can’t write it now because my train is coming.”

Fermat had a powerful intuition about such things, and many of his other conjectures (his Last was not really his last) later proved true. Mathematicians were quickly able to show that the assertion does indeed hold for cubes and fourth powers and then for many higher powers. At last count, solid proofs had ruled out any counterexamples for powers less than about 150,000.

But between 150,000 and infinity yawns a great gulf. And some superficially similar conjectures, at first seeming just as plausible as Fermat’s, have proved false. Leonhard Euler, for example, proposed in the 18th century that $a^4 + b^4 + c^4 = d^4$ had no nontrivial whole number solutions. In other words, no three perfect fourth powers add up to another perfect fourth power. For small numbers, Euler’s conjecture looked good. But just last summer, a Harvard mathematician, Noam Elkies, proved it wrong. One counterexample, found by Roger Frye of Thinking Machines Corporation in a long computer search, is $95,800^4 + 217,519^4 + 414,560^4 = 422,481^4$.

Meanwhile, the 20th century has brought the realization that just because a problem is genuine doesn’t mean it is solvable, even in principle. Kurt Gödel’s

Incompleteness Theorem has shown that any good system of logic—and mathematicians like to think of their universe as such a system—must have statements whose truth simply cannot be decided, one way or the other.

Confronted with the sad necessity of undecidable statements, many mathematicians were tempted to suspect that Fermat's theorem might be an example, doomed to remain forever in Gödel's limbo. Now that seems less likely. An American number theorist, Kenneth Ribet, proved last year that Fermat's theorem would follow from another, far less mysterious statement in mathematics—"a standard conjecture that everyone in the field believes in heart must be true," said Barry Mazur at the Institut des Hautes Études Scientifiques outside Paris.

At the very least, Dr. Ribet's work, and possibly Dr. Miyaoka's as well, makes Fermat's Last Theorem seem less isolated. "If it were false then we would have to revise our expectations about the structure of a certain field of mathematics," Dr. Mazur said, "and that wouldn't have necessarily been the case before."

So there is a suspicion in the air, a new intuition about the problem, a feeling that this leviathan may soon fall. In the currency of mathematics, though, suspicion, intuition and feeling don't always count for much.

April 17, 1988

At Last, Shout of "Eureka!" in Age-Old Math Mystery

By GINA KOLATA

More than 350 years ago, a French mathematician wrote a deceptively simple theorem in the margins of a book, adding that he had discovered a marvelous proof of it but lacked space to include it in the margin. He died without ever offering his proof, and mathematicians have been trying ever since to supply it.

Now, after thousands of claims of success that proved untrue, mathematicians say the daunting challenge, perhaps the most famous of unsolved mathematical problems, has at last been surmounted.

The problem is Fermat's Last Theorem, and its apparent conqueror is Dr. Andrew Wiles, a 40-year-old English mathematician who works at Princeton University. Dr. Wiles announced the result yesterday at the last of three lectures given over three days at Cambridge University in England.

Within a few minutes of the conclusion of his final lecture, computer mail messages were winging around the world as mathematicians alerted each other to the startling and almost wholly unexpected result.

Dr. Leonard Adleman of the University of Southern California said he received a message about an hour after Dr. Wiles's announcement. The frenzy is justified, he said. "It's the most exciting thing that's happened in—geez—maybe ever, in mathematics."

Impossible Is Possible

Mathematicians present at the lecture said they felt "an elation," said Dr. Kenneth Ribet of the University of California at Berkeley, in a telephone interview from Cambridge.

The theorem, an overarching statement about what solutions are possible for certain simple equations, was stated in 1637 by Pierre de Fermat, a 17th-century French mathematician and physicist. Many of the brightest minds in mathematics have struggled to find the proof ever since, and many have concluded that Fermat, contrary to his tantalizing claim, had probably failed to develop one despite his considerable mathematical ability.

With Dr. Wiles's result, Dr. Ribet said, "the mathematical landscape has changed." He explained: "You discover that things that seemed completely impossible are more of a reality. This changes the way you approach problems, what you think is possible."

Dr. Barry Mazur, a Harvard University mathematician, also reached by telephone in Cambridge, said: "A lot more is proved than Fermat's Last Theorem. One could envision a proof of a problem, no matter how celebrated, that had no implications. But this is just the reverse. This is the emergence of a technique that is visibly powerful. It's going to prove a lot more." Remember Pythagoras?

Fermat's Last Theorem has to do with equations of the form $x^n + y^n = z^n$. The case where n is 2 is familiar as the Pythagorean theorem, which says that the squares of the lengths of two sides of a right-angled triangle equal the square of the length of the hypotenuse. One such equation is $3^2 + 4^2 = 5^2$, since $9 + 16 = 25$.

Fermat's Last Theorem states that there are no solutions to such equations when n is a whole number greater than 2. This means, for instance, that it would be impossible to find any whole numbers x , y and z such that $x^3 + y^3 = z^3$. Thus $3^3 + 4^3 (27 + 64) = 91$, which is not the cube of any whole number.

Mathematicians in the United States said that the stature of Dr. Wiles and the imprimatur of the experts who heard his lectures, especially Dr. Ribet and Dr. Mazur, convinced them that the new proof was very likely to be right. In addition, they said, the logic of the proof is persuasive because it is built on a carefully developed edifice of mathematics that goes back more than 30 years and is widely accepted.

Experts cautioned that Dr. Wiles could, of course, have made some subtle misstep. Dr. Harold M. Edwards, a mathematician at the Courant Institute of Mathematical Sciences in New York, said that until the proof was published in a mathematical journal, which could take a year, and until it is checked many times, there is always a chance it is wrong. The author of a book on Fermat's Last Theorem, Dr. Edwards noted that "even good mathematicians have had false proofs."

Luring the World's "Crankers"

But even he said that Dr. Wiles's proof sounded like the real thing and "has to be taken very seriously."

Despite the apparent simplicity of the theorem, proving it was so hard that

in 1815 and in again 1860, the French Academy of Sciences offered a gold medal and 300 francs to anyone who could solve it. In 1908, the German Academy of Sciences offered a prize of 100,000 marks for a proof that the theorem was correct. The prize, which still stands but has been reduced to 7,500 marks, about \$4,400, has attracted the world's "cranks," Dr. Edwards said. When the Germans said the proof had to be published, "the cranks began publishing their solutions in the vanity press," he said, yielding thousands of booklets. The Germans told him they would even award the prize for a proof that the theorem was not true, Dr. Edwards added, saying that they "would be so overjoyed that they wouldn't have to read through these submissions."

But it was not just amateurs whose imagination was captured by the enigma. Famous mathematicians, too, spent years on it. Others avoided it for fear of being sucked into a quagmire. One mathematical genius, David Hilbert, said in 1920 that he would not work on it because "before beginning I should put in three years of intensive study, and I haven't that much time to spend on a probable failure."

Mathematicians armed with computers have shown that Fermat's theorem holds true up to very high numbers. But that falls well short of a general proof.

Tortuous Path to Proof

Dr. Ribet said that 20th-century work on the problem had begun to grow ever more divorced from Fermat's equations. "Over the last 60 years, people in number theory have forged an incredible number of tools to deal with simple problems like this," he said. Eventually, "people lost day-to-day contact with the old problems and were preoccupied with the objects they created," he said.

Dr. Wiles's proof draws on many of these mathematical tools but also "completes a chain of ideas," said Dr. Nicholas Katz of Princeton University. The work leading to the proof began in 1954, when the late Japanese mathematician Yutaka Taniyama made a conjecture about mathematical objects called elliptic curves. That conjecture was refined by Dr. Goro Shimura of Princeton University a few years later. But for decades, Dr. Katz said, mathematicians had no idea that this had any relationship to Fermat's Last Theorem. "They seemed to be on different planets," he said.

In the mid-1980s, Dr. Gerhard Frey of the University of the Saarlands in Germany "came up with a very strange, very simple connection between the Taniyama conjecture and Fermat's Last Theorem," Dr. Katz said. "It gave a sort

of rough idea that if you knew Taniyama's conjecture you would in fact know Fermat's Last Theorem," he explained. In 1987, Dr. Ribet proved the connection. Now, Dr. Wiles has shown that a form of the Taniyama conjecture is true and that this implies that Fermat's Last Theorem must be true.

"One of the things that's most remarkable about the fact that Fermat's Last Theorem is proven is the incredibly roundabout path that led to it," Dr. Katz said.

Another remarkable aspect is that such a seemingly simple problem would require such sophisticated and highly specialized mathematics for its proof. Dr. Ribet estimated that a tenth of one percent of mathematicians could understand Dr. Wiles's work because the mathematics is so technical. "You have to know a lot about modular forms and algebraic geometry," he said. "You have to have followed the subject very closely."

The general idea behind Dr. Wiles's proof was to associate an elliptic curve, which is a mathematical object that looks something like the surface of a doughnut, with an equation of Fermat's theorem. If the theorem were false and there were indeed solutions to the Fermat equations, a peculiar curve would result. The proof hinged on showing that such a curve could not exist.

Dr. Wiles, who has told colleagues that he is reluctant to speak to the press, could not be reached yesterday. Dr. Ribet, who described Dr. Wiles as shy, said he had been asked to speak for him.

Dr. Ribet said it took Dr. Wiles seven years to solve the problem. He had a solution for a special case of the conjecture two years ago, Dr. Ribet said, but told no one. "It didn't give him enough and he felt very discouraged by it," he said.

Dr. Wiles presented his results this week at a small conference in Cambridge, England, his birthplace, on "P-adic Galois Representations, Iwasawa Theory and the Tamagawa Numbers of Motives." He gave a lecture a day on Monday, Tuesday and Wednesday with the title "Modular Forms, Elliptic Curves and Galois Representations." There was no hint in the title that Fermat's Last Theorem would be discussed, Dr. Ribet said.

"As Wiles began his lectures, there was more and more speculation about what it was going to be," Dr. Ribet said. The audience of specialists in these arcane fields swelled from about 40 on the first day to 60 yesterday. Finally, at the end of his third lecture, Dr. Wiles concluded that he had proved a general case of the Taniyama conjecture. Then, seemingly as an afterthought, he noted that that meant that Fermat's Last Theorem was true.

Q.E.D.

People raised their cameras and snapped pictures of this historic moment, Dr. Ribet said. Then "there was a warm round of applause, followed by a couple of questions and another warm round of applause," he added.

"I had to give the next lecture," Dr. Ribet said. "It was something incredibly mundane." Since mathematicians are "a pretty well behaved bunch," they listened politely. But, he said, it was hard to concentrate. "Most people in the room, including me, were incredibly shell-shocked," he said.

June 24, 1993

Fermat's Theorem

By JAMES GLEICK

We've learned a thing or two. We know we live in a small corner of an expanding universe. We know that matter is made of atoms. We know that absolute truth is hard to come by. And now we know—having spent three and a half centuries on it—that no number cubed can be the sum of two other cubed numbers, nor any fourth power the sum of two fourth powers, nor any higher power the sum of two like powers.

What a peculiar bit of knowledge! Yet if anyone is out there judging the galaxy's civilizations according to some handbook of "What Every Bright Species Ought to Know," it seems reasonable to suppose that somewhere on the list will be the fact of arithmetic that we call Fermat's Last Theorem. It must be a universal truth—true here, true everywhere, true now, true always.

On our planet, however, and maybe on other planets as well, proof was long in coming. Three hundred fifty-six years have passed since the Frenchman Pierre de Fermat, lawyer and councilor in Toulouse, just beginning a series of explorations that marked the creation of modern number theory, defaced his beloved copy of Diophantus's *Arithmetic* with a bold assertion: no whole number solutions exist for the statement $x^n + y^n = z^n$, where n is greater than 2. Startling, because when n does happen to be 2, the equation has an infinity of easy-to-find solutions: 3 squared (9) plus 4 squared (16) equals 5 squared (25), as every high school geometer knows; 5 squared (25) plus 12 squared (144) equals 13 squared (169).

Fermat's Last Theorem has been a sore spot—a gaping, hideous, vacant lot sitting smack in the middle of downtown while the elegant and gaudy towers of modern mathematics have risen all around. No wonder a veritable battalion (as *Notices of the American Mathematical Society* reports) of "more than 60 mathematicians, a fair number of them carrying cameras," having heard rumors, descended on the last in a series of lectures by Prof. Andrew Wiles at Cambridge University in June, undaunted by Wiles's shrewdly modest title, "Elliptic Curves, Modular Forms and Galois Representations." At the end, in an only moderately obscure way, Wiles gave them what they had been hoping for: F.L.T., Q.E.D.

Saved by the Margin

Fermat glossed his assertion with a famous remark that must have seemed so harmless as he penned it, yet has been a razor thorn in the brains of number theorists ever since: "I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain."

Marvelous. Whole branches of mathematics have been born of failed proofs of Fermat's Last Theorem—his last, by the way, not because it was the last he stated but because it was the last remaining to be confirmed. And not just mathematicians, but interested children and imaginative cranks have been plugging away ever since, no doubt realizing that if they didn't have Fermat's raw genius at their disposal, they nevertheless had more paper. Hence the mathematicians' form letter to cranks who submit their perennial proofs: "I have an elegant refutation of your attempted proof, but unfortunately this page is not large enough to contain it." Or for that matter, the graffito scrawled in an Eighth Avenue subway station a few summers ago: "I have discovered a truly remarkable proof, but I can't write it now because my train is coming."

A half-dozen or dozen people on earth have some hope of understanding Wiles's proof from start to finish, and most of those people are now hard at work on it as referees. All the early returns suggest that this is the real thing.

"Think of it this way," says Barry Mazur of Harvard University, one of several number theorists who contributed rungs to the ladder Wiles climbed. "This was a technical statement scrawled in the margin of a book 356 years ago. Of course, Wiles's proof uses modern techniques. But the problem was answered strictly in its own terms. That's rather amazing right there. It underscores how stable mathematics is through the centuries—how mathematics is one of humanity's long continuous conversations with itself."

Isn't He Too Old for All This?

Wiles has had the ill grace to turn 40 years old—exactly the age, according to an unwritten rule, at which he loses eligibility for the most prestigious prize in mathematics, the Fields Medal. Thus, mathematics faces a new quandary. Just how rigorous is this rule? Would it not embarrass the prize-givers more than the potential recipient to overlook an achievement of this magnitude?

Wiles, an Englishman now settled in Princeton, N.J., retreating slightly

behind his wire rims, has nothing to say about these trappings of celebrity. He has bemusedly turned down a \$750 invitation to pose in a Gap advertisement—although, in his khakis, pale blue open-neck shirt and white New Balance sneakers, he looks as though he wouldn't even have had to change. Nevertheless, he is delighted to have broken another of his profession's unwritten rules: that great mathematics is performed only by the young.

"If I've helped to counter that idea, I'm very happy," Wiles says. There is no real reason, he is sure, that the elderly of mathematics—the 30-somethings and even 40-somethings—cannot do powerful and creative work. No reason, that is, to do with the quality of their mental machinery.

"When you're young, you feel you can do anything," Wiles says. "You don't have any feeling for what your limitations are. I think it's more this psychological change as you get older. You realize how hard problems are. You've had some sort of research record and you know what sort of problems you've solved, and you probably don't try ones that are much harder."

Translation, Please

As the words wash over you, you can almost feel that the mathematicians are speaking English; if you could only get your mind to stop wandering for a second, you might be able to follow the boiled-down explanation provided by Kenneth A. Ribet, a mathematician at the University of California at Berkeley who with a remarkable piece of work seven years ago provided the launching pad for Wiles's proof. "You use Hilbert irreducibility and the Cebotarev density theorem (in some way that hasn't yet sunk in)"—you can say that again—"to produce a non-cuspidal rational point of X over which the covering remains irreducible." Oh, yes! The covering . . . just remind me?

It's slightly heartwarming to discover that your normal everyday mathematician also has trouble following this. Here we are at teatime in Fine Hall, Princeton—a venerable mathematics department tradition dating back past the era when Albert Einstein might be among those dropping by. A couple of distinguished professors welcome Wiles at their table, and one of them takes the opportunity to get to the heart of the matter. What is the Taniyama conjecture, exactly?

Wiles flashes me a look—I asked him the same question not a half-hour before, and now, instead of the Dr. Seuss version he tossed my way, I'm going to hear something closer to the real thing. He speaks, and his listeners nod gamely.

Nevertheless, I have the impression that they, too, need a bigger mitt if they want to field this one safely.

That's all right. They can always wait for Ribet's explanation: "Taniyama's conjecture states that for each such surface S there is a congruence subgroup of $SL(2, \mathbb{Z})$ and a nonconstant analytic map from X to S where X is the quotient of the complex upper half-plane by the congruence subgroup."

It's an impressively economical way of speaking, really—a picture's-worth-a-thousand-words approach wherein one word is worth a thousand words. Never mind that the published version of Wiles's proof will run 200 pages. To expand the shorthand, flesh it out so that, say, Fermat could understand it, would require many times more.

It seems easier to summarize difficult results from physics, where at least the chain of obscure language leads to things that are, somehow, real. What did these mathematicians prove? Yutaka Taniyama and successors made a connection between a class of equations called elliptic curves (never mind exactly what they are) and another, very special class called modular curves (never mind exactly what they are).

Ribet, building on the work of Gerhard Frey and Jean-Pierre Serre, showed seven years ago that this meant that if there were a counterexample to Fermat's Last Theorem, then it would be possible to construct an elliptic curve that was not modular. Enter Wiles. He showed that the Taniyama conjecture must be true for elliptic curves with "square-free conductors" (n.m.e.w.t.a.)—and so on. . . .

What Can't We Solve?

"We evolved from this universe," says Simon Kochen, Wiles's department chairman at Princeton. "And our brains work in some kind of conformity with the universe. There must be some kind of harmony between the way we think and the way the universe works."

Sifting through the congratulatory mail, both paper and electronic, that pours into his office daily, Wiles encounters his well-wishers' joy that the problem has been solved during their lifetimes. "They are happy," he says, "because it really had seemed very likely to many people that they would die without knowing whether there was a solution."

Many *Star Trek* fans, however, are concerned. It seems that Captain Jean-Luc Picard has already been shown, centuries hence, trying to solve the "unsolved"

Fermat's Last Theorem. So Wiles, while livening up our history, has rather inconveniently violated *Star Trek's*. And the writers normally try to stay so close to reality!

Ours was, after all, the century of Kurt Gödel and "undecidability," the century when mathematics discovered that some statements of pure arithmetic or logic can never be proved true or false. Mathematics-watchers naturally wondered whether they already had a real live case of Gödel undecidability in Fermat's Last Theorem. Martin Gardner, the well-known recreational mathematics writer, said a few years ago that he believed and hoped so. "This leads to a dismal (though to me, delightful) possibility," he wrote. "Mathematicians and their supercomputers will forever struggle with the theorem, never finding a counter example, never knowing for sure if it is true and never giving up because, like the mountain, it's there."

Yet Wiles himself never considered the possibility. He believed, and believes, that simple-to-state problems about properties of numbers must be solvable. Not only that, he believes they must be solvable by human beings—that is, by any old garden-variety number theorist.

If so, perhaps it is partly because of a change in the way our species operates these days. It subtracts nothing from Wiles's determined seven-year achievement to note that it came not just from an individual but from a community, a social organism far different from Fermat's community of a few scattered, part-time gentlemen exchanging speculation by slow post. Mathematics today is huge, fast, professional, electric. It relies on lines of almost instantaneous wired communication; on a highly refined understanding of what proof is and how it works; on a vast and sprawling edifice of accumulated knowledge.

So Wiles drew on distant strands of thought. The sources listed by Andrew Granville, another mathematician who has worked on the problem, is a United Nations smorgasbord: "... L-functions, group schemes, crystalline cohomology, Galois representations, modular forms, deformation theory, Gorenstein rings, Euler systems. . . . Britain, France, Germany, Italy, Japan, the United States, Canada, Russia, Brazil, Australia and Colombia." No wonder Wiles finds himself in an optimistic frame of mind.

The idea that some problem of basic number theory might just be too hard for a species like ours—as Fermat's Last Theorem is too hard for, say Labrador retrievers—Wiles is not willing to credit. We've got the ability, he says. Just give us enough time.

October 3, 1993

Flaw Is Found in Math Proof, but Repairs Are Under Way

By GINA KOLATA

The widely heralded proof of Fermat's Last Theorem, one of the most enduring and difficult problems in mathematics, has hit a snag in the review process before publication, the proof's discoverer said this week. But he said he did not believe it was a fatal flaw.

Others said such problems were to be expected when a long and extremely complex proof undergoes rigorous scrutiny before publication. They said it would be premature to conclude that the proof is in trouble.

Mathematicians around the world were stunned when Dr. Andrew Wiles of Princeton University announced in June that he had a proof of Fermat's Last Theorem. The theorem had been stated 356 years ago by a French mathematician and physicist, Pierre de Fermat, who scrawled it in the margin of a book, adding that he had a marvelous proof but that the margin was too small to hold it.

The theorem was tantalizingly simple, a statement about what sorts of solutions were possible for certain elementary equations. But it thwarted even the best mathematical minds until Dr. Wiles came forward.

Fermat's theorem involves equations of the form $x^n + y^n = z^n$. When n is 2, this is the Pythagorean theorem, which states that the sum of the squares of the lengths of the sides of a right triangle equal the square of the length of the hypotenuse.

Fermat proposed that there were no solutions to the equations when n is a whole number greater than 2.

40 Years of Research

Dr. Wiles's proof that Fermat was correct drew on 40 years of mathematical research involving abstractions that seemed completely removed from the equations of Fermat's theorem. But because the logic and structure of the proof were so compelling, because Dr. Wiles had a reputation as a gifted and careful researcher, and because the groundwork for the proof lay in recent but well-accepted discoveries, mathematicians hailed the proof as almost certainly correct.

The next step was the checking, the sifting through the proof for errors or omissions. Dr. Wiles submitted his 200-page manuscript to the journal *Inventiones*

Mathematicae, which is edited by Dr. Barry Mazur of Harvard University. Dr. Mazur sent the paper to six reviewers, who began looking assiduously for places where the logic was unclear or where further explanations were needed.

As the reviewers found such rough spots, Dr. Wiles immediately smoothed them out, with one exception. That is a problem involving the calculation of a precise upper limit of a mathematical object called the Selmer group in the semistable case. But in a statement sent out by electronic mail and released by Princeton University, Dr. Wiles wrote, "I believe that I will be able to finish this in the near future." He added that he "will give a full account of this work," in lectures on Fermat's Last Theorem at Princeton in February.

Dr. J. J. Kohn, chairman of Princeton's mathematics department, said, "It would be really premature to say that he doesn't have a proof."

Dr. Kenneth Ribet, a mathematician at the University of California at Berkeley who is one of the best qualified to assess the significance of the missing step in the proof, is sanguine. Dr. Ribet, whose own work was crucial to Dr. Wiles's proof, said Dr. Wiles had "a strategy, an overarching plan," adding: "There are lots of individual steps, and one step is not sufficiently justified. But it is very, very likely to be true."

Dr. Ribet said large, complex proofs often had subtle missing steps that can be corrected. "The probability of a snag in a proof like this is very, very high," he said.

Jealously and Feeds Gossip

But even the hint of a snag in Dr. Wiles's proof has set off wild rumors in the world of mathematics, behavior that Dr. Kohn characterized as ungentlemanly.

Mathematicians say the rumors spread in part because stakes are high and professional jealousy may be keen. But they add that rumors have also been fueled by Dr. Wiles's decision not to release his proof until it is absolutely correct and ready for publication, leaving mathematicians to speculate about the details.

In contrast, Dr. Ribet said, when he made his major discovery he lectured on it repeatedly and passed out copies of it, asking colleagues for help in spotting errors. "People would point out things they didn't feel comfortable with," he said. "There were a couple of points where I got caught and I had to work really furiously."

Dr. Wiles, however, shut himself up in his attic for seven years to work on his proof in absolute secrecy. He has still not circulated drafts of his manuscript, and mathematicians feel excluded. "It's a little frustrating to people," Dr. Ribet said.

December 11, 1993

A Year Later Fermat's Puzzle Is Still Not Quite Q.E.D.

By GINA KOLATA

One year after a Princeton mathematician convinced the world that he had proved the most famous unsolved math problem, the much-touted proof has entered a realm of mathematical limbo. The proof, by Dr. Andrew Wiles of Princeton University, said that a 357-year-old problem, known as Fermat's Last Theorem, was true.

The theorem states that equations of the form $x^n + y^n = z^n$ only have solutions when the exponents are whole numbers smaller than 3. Pierre de Fermat, a French physicist and mathematician, had scribbled the problem in the margin of a book, saying that he had a marvelous proof but the margin, alas, was too small to hold it.

Ever since, thousands of professional and amateur mathematicians have searched for a way to show that the theorem is true. Mathematicians said that Dr. Wiles's lengthy proof, which didn't come close to fitting in a margin, had the ring of truth when he announced it last year. Although it used new methods that pushed the limits of what mathematics can do, it built on decades of work by others and seemed to follow a compelling logic.

Dr. Wiles, who devised the proof after working in solitude in his attic office for seven years, claimed to have proved a much larger and theoretically more important result, called the Taniyama conjecture. And, others had shown, if the Taniyama conjecture is true, so is Fermat's theorem.

But when Dr. Wiles sent his proof to a mathematics journal for review prior to publication, one of the reviewers found a gap that Dr. Wiles has, as yet, been unable to fill. Such gaps are to be expected in long and technical proofs, and mathematicians say they cannot tell whether the gap is a fatal blow or a temporary hurdle to the final proof.

The first half of the proof, which is correct, is a momentous achievement in its own right, mathematicians say. But unless the entire proof is completed, Fermat's theorem will remain unproved. And Fermat will continue to have his last chuckle from the grave.

July 3, 1994

How a Gap in the Fermat Proof Was Bridged

By GINA KOLATA

Fermat's Last Theorem, which has tantalized mathematicians for more than 350 years, has at last been solved, say those who have read the revised but not yet published proof. But the endgame of this furious chase has proved as full of last-minute surprises as a murder mystery.

For Dr. Andrew Wiles of Princeton University, the chief author of the proof, triumph had to be snatched from the jaws of disaster. His first proof, which aroused worldwide attention when announced two years ago, turned out to contain a gap, which Dr. Wiles found he was unable to cross alone.

The enormous intellectual trophy of having conquered the world's most famous mathematical problem seemed about to slip from his grasp. If he invited a well-known mathematician to help him bridge the gap, he would risk having to share the credit. What was needed, and what he pulled off, was a miraculous save with just the right collaborator.

On a mathematical level, Fermat's Last Theorem turns out to have extraordinarily deep roots, despite its apparent simplicity. The theorem is a special case of an overarching mathematical idea known as the Taniyama conjecture, which is itself a giant step toward the goal of the Langlands program, a grand unified theory of mathematics.

Proving Fermat's theorem showed how the even more daunting Taniyama conjecture might be tackled and now, with Dr. Wiles's proof in hand, one of his former students, Dr. Fred Diamond of Cambridge University in England, has already made considerable progress on the conjecture.

Fermat's Last Theorem dates to 1637. The French mathematician and physicist Pierre de Fermat had scribbled it in the margins of a book, adding that he had discovered a marvelous proof but that the margins were too small to hold it.

The theorem says that equations of the form $x^n + y^n = z^n$ have no solutions when n is a whole number greater than 2 and when x , y and z are positive whole numbers. When n equals 2, the equation is the familiar Pythagorean equation, which says that the squares of the lengths of two sides of a right triangle equal the square of the length of its hypotenuse. One solution is $3^2 + 4^2 = 5^2$.

Dr. Wiles, who is 41, had been fascinated with the challenge of the theorem since he was a child. Indeed it was Fermat's Last Theorem that drew him into

mathematics. But he did not begin working on his proof until eight years ago, secluded in his attic office and telling just a few trusted friends what he was doing. Finally, he convinced himself that the work was done and he announced it in a series of three lectures at a mathematics meeting in Cambridge, England. Only at the end of the third lecture, on June 24, 1993, came the stunning announcement—Fermat's Last Theorem was proved.

Leading researchers immediately hailed Dr. Wiles's achievement. Built on a body of sophisticated mathematics that had been developed in recent years, his proof made so much sense that they confidently predicted it would hold up to scrutiny.

Dr. Wiles, cautious and a bit nervous, decided not to circulate copies of his manuscript widely among mathematicians but instead to wait until a select few experts who were reviewing it before publication proclaimed it sound. Writing a complex proof, he said, "is like writing in a foreign language—you are bound to make a few grammatical errors." If there were any faults, as often happens with complicated proofs, he wanted to fix them himself rather than share the glory.

"It's a very competitive environment," Dr. Wiles explained, and, after working for seven years and after getting so close, he wanted the victory to be his alone.

The Gap: A "Minor" Problem Turns into a Crisis

Several minor faults were found and Dr. Wiles fixed them. But then, in the fall of 1993, a reviewer asked him to justify an assertion, in the midst of his proof, that a certain estimate was correct.

The gap at first seemed to be a minor one. But though the estimate seemed intuitively to be correct, proving it was a different matter.

"At first I thought I was just being slow," he said. "It can be very hard to tell at first whether you're just being blind to something or whether there really is an obstacle—it's very hard to tell the difference." After struggling in vain, he decided to go into complete seclusion. "If I was to focus on the problem, I could not allow myself to be distracted," he said. He tried out ideas on a Princeton colleague, Dr. Nicholas Katz, but told no one else the details of what he was doing.

In the outside world, Dr. Wiles's secretiveness irritated many and touched off a betting game on what he was up to and whether he would succeed.

"I noticed he was stuck and I was very pessimistic," said Dr. Gerd Faltings, a mathematician at the Max Planck Institute in Bonn, Germany.

Dr. Kenneth Ribet of the University of California at Berkeley said that although he was rooting for Dr. Wiles, as time went by the unfilled gap in the proof was becoming something of an embarrassment. "A proof that is unfinished is no proof at all," Dr. Ribet said. "I had heard from people in other parts of mathematics that this whole algebraic geometry group has egg on its face, that we can't get our act together. They would say that we don't know a proof when we see one, so how could anyone believe what we say."

Unfortunately, Dr. Wiles said, the gap had turned up in the very part of the proof where he felt he was on the shakiest ground. He had used a new and powerful method devised by Matthias Flach of Princeton University. But, Dr. Wiles said, Dr. Flach's method, "used a lot of sophisticated machinery, and I didn't feel completely comfortable with it."

As months went by, Dr. Wiles finally decided that he needed help. He was frightened that he would mislead himself, spending years, or decades, going in circles trying frantically to fix the gap with methods that never would work. "There are people who have spent 30 years on one problem," he said. "You get caught in problems, trapped in them. I knew the danger, psychologically."

And it was getting harder and harder to think clearly. "I was very tired," he said. "I'd been working very hard, and I needed someone to check every statement I made. I needed someone to talk to all the time." But Dr. Wiles needed a collaborator who would allow him to call the shots. "I wanted to choose the direction—I didn't want someone to come in with lots of new methods," Dr. Wiles said. Before he gave up and let the world in on the problem, he said, "I wanted to make sure that I had completely explored the ideas that I had and that I hadn't missed something obvious."

The glory of being the person to have proved the theorem was too overwhelming to give up without a fight. Dr. Wiles quoted Enrico Bombieri, a mathematician at the Institute for Advanced Study in Princeton, who said: "Everyone has their price. For mathematicians, it's Fermat's Last Theorem or the Riemann hypothesis." Riemann is another outstanding unsolved problem.

Dr. Wiles thought carefully about whom he would ask to join him. "I wanted someone I was sure of," he said. So he called Dr. Richard Taylor, 32, a former student who is now a reader, a tenured position, at Cambridge University.

Dr. Taylor said he was surprised and excited when Dr. Wiles called him in December 1993 to ask for help. He had a sabbatical coming up, so he arrived in Princeton last January ready to work intensively on the problem. While Dr.

Wiles had “extremely good” intuition, Dr. Taylor said, “I’m somebody who is more concerned with details.”

Dr. Wiles and Dr. Taylor spent several months trying to see whether Dr. Flach’s methods could be made to work. Then, over the summer, they tried a different approach, one that was a long shot, in Dr. Wiles’s opinion. Finally, Dr. Taylor suggested that they go back to Dr. Flach’s method once again. Dr. Wiles was reluctant. “I confess that at that time I was thinking that it would need a whole new approach that would take several years and require many people,” he said.

But he went back to the Flach method for one last time. “There was one variant in the original argument that I’d convinced myself wouldn’t work but I hadn’t convinced him,” Dr. Wiles said. “I was sitting at my desk one morning really trying to pin down why the Flach method wasn’t working when, in a flash, I saw that what was making it not work was exactly what would make a method I’d tried three years before work. It was totally unexpected. I didn’t quite believe it.” He dashed down from the attic to tell his wife. Although his enthusiasm was infectious, Dr. Wiles said, “I actually think she didn’t believe me.”

Dr. Wiles tried to control his mounting elation. “I was too excited to think clearly,” he said. “I slept on it,” he said, and in the morning he called Dr. Taylor, who, by this time had returned to England. The two began collaborating furiously and, two and a half weeks later, they had written a paper, whose authors are Dr. Wiles and Dr. Taylor, that filled in the gap of the proof.

The credit for solving Fermat’s Last Theorem seems likely to go largely to Dr. Wiles, since he is the sole author of the major paper on the proof, and since it was his ideas that bridged the gap. Although Dr. Taylor evidently played an important supporting role, he says that he agrees with Dr. Wiles’s account of their collaboration. Dr. Diamond carefully describes the proof as “the theorem of Wiles, completed by Taylor and Wiles.” Dr. Wiles said he agreed with this description.

The Breakthrough: Discovering Gold in “Pigeonholes”

Dr. Wiles said that the breakthrough came in figuring out how to glue together an infinite collection of mathematical objects called Hecke rings. He had initially been creating what was “a very natural relationship between these objects—natural in the sense that you can give a clear definition of the maps between them.” It was an inductive argument. The idea was to take one element of a set and use that to find the next element, then to use the second to construct a third, and so on.

The new idea, Dr. Wiles said, "was to simply construct artificial maps between these objects."

"You wouldn't show a relationship explicitly," he said, but would use a counting argument to prove that a relationship had to exist. The basic idea is to use the pigeonhole principle: if you have more objects than pigeonholes to put them in, then at least one pigeonhole must contain more than one object.

The complete argument involves creating an infinite sequence of sets of pigeonholes and then showing that there must be objects that show up in every set of pigeonholes. This allowed Dr. Wiles and Dr. Taylor to prove that there must be an infinite set of Hecke rings that share a relationship, although they never have to specify exactly what that relationship is.

Before Dr. Wiles was willing to announce that he and Dr. Taylor had filled the gap, he asked a few leading experts to check his argument. One was Dr. Faltings in Germany, who said he read it in a week and was convinced it was correct. Now, Dr. Faltings has improved the proof, making it sleeker and easier to follow. Still, he said, most mathematicians who are expert enough in the field to read the proof will probably require a month to go through it.

Another who got the proof early was Dr. Diamond, 30. "I certainly didn't expect that kind of argument," Dr. Diamond said. "It's so ingenious."

A few weeks later, he discovered how to extend it to prove a larger section of the Taniyama conjecture. The conjecture involves elliptic curves defined over the rational numbers. Dr. Wiles and Dr. Taylor showed it was true for a subset of elliptic curves, including those known as semistable curves. Dr. Diamond showed it was true for a much larger group of elliptic curves.

The Next Frontier: On to Taniyama; Then Langlands?

Now, mathematicians said, the final proof of the elusive Taniyama conjecture is in sight. "If I had to guess, I would say it is at least a few months and at most a few years," before the entire conjecture is proved, Dr. Diamond said.

Dr. Michael Rosen of Brown University said that Dr. Wiles's ideas have proved "ground-breaking." The Taniyama conjecture had seemed beyond researchers' reach. No one had any idea how to prove it. "People were saying, 'Maybe in another 30 or 40 years,' it would be proved," Dr. Rosen noted.

And, finally, the work is a major step in the Langlands program, the grand unified theory of mathematics. Dr. James Arthur of the Institute for Advanced

Study in Princeton said the Langlands program, a conjecture proposed a quarter-century ago by Dr. Robert Langlands, united two seemingly disparate fields of mathematics. It says that the mathematics of algebra, which involves equations, and the mathematics of analysis, which involves the study of smooth curves and continuous variations, are intimately related.

The conjectures in the Langlands program "are like a cathedral, the way they fit together so beautifully," Dr. Arthur said. Yet, he said, "they are so difficult to prove."

"The only way to prove them seems to be by very, very indirect means," he said, adding that he thought it would take "decades at the very least, maybe centuries," to complete the Langlands program.

Nonetheless, Dr. Arthur said, the greatest advance so far has been the work of Dr. Wiles and Dr. Taylor and the recent result by Dr. Diamond. "It was an enormous accomplishment, what Wiles has done, really a huge step," Dr. Arthur said.

Dr. Wiles does not intend to work on the Langlands program, and he has no intention of extending his proof or mining it for new results. "It is nice to finish it off, but, for me, the mystery is gone," he said. "The challenge now is to go on to problems where no one has any idea where to start."

For now, Dr. Wiles is taking a break, getting back to his mail, talking to people again. He had worked for so long and so hard on the problem that it is difficult to realize that finally it is done. "Sometimes it's hard to wake up," he said. "I have to remind myself that it's all over."

So what will he work on next? Ever elusive, Dr. Wiles said that was one thing he would never reveal.

January 31, 1995

Two Key Mathematics Questions Answered after Quarter Century

By JOHN A. OSMUNDSEN

Two of the most fundamental important questions in mathematics today have been answered by Paul J. Cohen, a young Stanford University mathematician.

The two questions had persisted for more than a quarter century. By answering them, Dr. Cohen demonstrated the power of modern mathematics. Ironically, he exposed some of its weakness as well.

The proof, which will be published soon, concerns a branch of mathematics known as the theory of sets, which deals with collections of things. Dr. Cohen's work has meaning, however, for the foundations of all mathematics.

The theory of sets was developed by Georg Cantor, a German, in 1871. Today, it provides part of the basis for the so-called "new mathematics" that is being taught in many elementary and high schools across the country.

The idea behind the use of set theory as a teaching aid in beginning mathematics is that concepts such as those of numbers, counting and arithmetic can be more easily understood by seeing how things can be grouped together and how various collections of things are related to one another than by the rote learning of rules.

Called Research Tool

Moreover, set theory serves as a powerful research probe into the foundations of mathematics. In fact, one mathematician observed recently that all of mathematics could be expressed in terms of theory of sets.

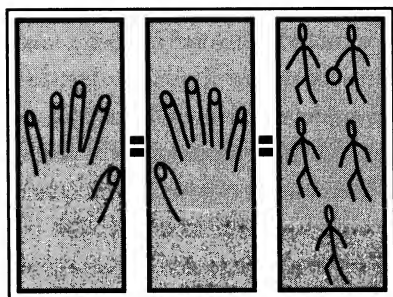
A brief introduction to set theory and the contribution to it made by Dr. Cohen were presented at a seminar on mathematics for science writers recently by Prof. Raymond M. Smullyan of Yeshiva University.

The seminar was held at Columbia University under the auspices of the Society for Industrial and Applied Mathematics and the Martin Company's Research Institute for Advanced Studies. The following is how Professor Smullyan explained things.

A set is a collection of things—numbers, points on a line, various objects, and so forth. An important characteristic of a set is the number of things it contains.

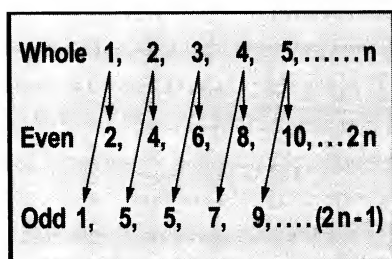
This is called the set's cardinal number. All sets whose elements can be put into one-to-one correspondence with the elements of each other are said to be equivalent and have the same cardinal number.

For example, the set consisting of the fingers on the left hand is equivalent to the set of fingers on the right and to the set of men on a basketball team because the elements of each set can be put into a one-to-one relationship with those of each of the others. Their common cardinal number is five.



Those sets would not be equivalent, of course, to the set of dimes in a dollar or the set of wheels on a car, because the cardinal numbers of those sets are 10 and 4, respectively.

These are infinitely larger sets too. The set of all whole numbers—that is, those without fractions (0, 1, 2, 3, etc.)—is an example of an infinite set. It is equivalent to the set of all even numbers because, for every whole number, it is possible to find an even number to correspond. For the same reason, the set of all odd numbers and the set of all pairs of whole numbers is, each, equivalent to the set of all whole numbers.



Cantor gave the name of “aleph-null” to the cardinal number sets of all such finite numbers (0, 1, 2, 3, 4, etc.). It might seem that all infinite sets would have this same cardinal number, but Cantor showed otherwise.

He showed, first, that such sets as the set of all real numbers between zero and one (decimals, that is), the set of all points on a line and the collection of all sets of whole numbers have a higher cardinal number than aleph-null. He called this cardinal number “c,” for the “power of the continuum.”

Cantor showed that the cardinal number, c, is higher than aleph-null by the following sort of proof.

Proof Is Outlined

Make a collection of all conceivable sets of whole numbers such that, arbitrarily, Set 1 might contain all numbers between 10 and 50, Set 2 might have all even numbers between 1 and 25, Set 3 all numbers between 36 and 92, etc.

Next, match each set with each whole number in the set of all whole numbers so that Set 1 goes with "one," Set 2 with "two," etc.

Now, make a new set of whole numbers in an orderly way by putting the number "one" into this new set if the first set does not contain "one" or leaving "one" out if the first set has it, putting number "two" into the new set if the second set does not have it or leaving "two" out of the new one if that number is in the second set, etc.

The result will be a set of whole numbers that differs from each of the other sets in the collection by at least one number. This new set, of course, must belong to the collection of all sets of whole numbers. But that collection had been put into the one-to-one correspondence with the set of all whole numbers (cardinal number, aleph-null) before the new set was constructed.

Therefore, the resultant collection of sets of whole numbers—including the newly constructed set—is larger than the whole number set and must have a higher cardinal number, c , than aleph-null.

Cantor then went on to show that there are infinitely many cardinal numbers that can be arranged in an ascending sequence.

That this is so followed from Cantor's demonstration that the collection of subsets of any set is larger than the set itself. This principle is obvious for finite sets. The subsets of a three-element set of such figures as 1, 2, 3, for example, are 1; 2; 3 (all one-element subsets); 1, 2; 1, 3; 2, 3 (all two-element subsets); 1, 2, 3 (the set itself); and an empty set—or eight in all. Cantor showed this was true for infinite sets as well.

SET			
1	2	3	= 3 elements (Cardinal number 3)
SUBSETS			
1	2	3	
1,2	1,3	2,3	
1,2,3			= 8 elements (Cardinal number 8)

This situation gave rise immediately to a fundamental question involving set theory. If aleph-null is the smallest cardinal number for an infinite set, and there are infinitely many such cardinal numbers, what is the second smallest cardinal number of this sort? Particularly, is c the next higher one after aleph-null?

In other words, is there a collection of things that is larger than the collection

of all whole numbers (cardinal number, aleph-null) but smaller than the collection of all sets or the collection of all points in a line (cardinal number, c)? Or is there an intermediate-sized set with a cardinal number between aleph-null and c ? This has become known as the "continuum problem" or the "continuum hypothesis."

In 1938, Kurt Gödel of the Institute for Advanced Study in Princeton proved that the continuum hypothesis could not be disproved with the existing axioms of set theory. He did this by showing that the continuum hypothesis was true under a new definition of the word "set" by which all axioms of the set theory held true, also.

This left the question open, however, whether there were other consistent models of set theory in which the continuum hypothesis would be false. In other words, could the continuum problem be solved at all with the axioms of set theory?

It is this fundamental question that Dr. Cohen has now answered. He found another model of sets that satisfied all the axioms of the theory but under which the continuum hypothesis was untrue. Thus, the existence of an intermediate cardinal number between aleph-null and c cannot be proved with set theory as it now stands, and the continuum problem will remain a problem until some fundamentally new axioms are invented.

"Axiom of Choice" Tested

In the course of producing that proof, Dr. Cohen answered another fundamental question. It concerned the "axiom of choice," one of the most important tools in mathematics.

This axiom states that it is possible to take one element out of each set in a collection of sets and make a new set from them.

This may seem on the surface to be self-evident. Yet, it has never been proved, and mathematicians would like to prove it because this axiom is so universally applied. Some years ago, Bertrand Russell gave an illustration of the necessity for the axiom.

One can make a new set of shoes from a set of pairs of sets by extracting one shoe from each pair without deciding each time which shoe to take: simply order all left shoes (or all right shoes). This cannot be done with a set of pairs of socks, however, because there are no left or right socks. Thus, a choice between the socks in each pair must be made each time for the construction of a new set.

Professor Gödel also worked on this problem and was able to show that the axiom of choice could not be disproved with set theory. Again, however, the question remained whether the axiom could be proved.

This is the second fundamental question that Dr. Cohen has answered. He has shown that the axiom of choice cannot be proved, either, with set theory.

"More important still," Professor Smullyan remarked in this connection, "is that Cohen has shown that the continuum problem cannot be solved even with the use of the axiom of choice."

"Thus," he said, "the most powerful set of reasonable axioms we have at our disposal is insufficient to settle another problem one way or another."

November 14, 1963

Mathematical Theory of Poker Is Applied to Business Problems

By WILL LISSNER

A new approach to economic analysis that seeks to solve hitherto insoluble problems of business strategy by developing and applying to them a new mathematical theory of games of strategy like poker, chess and solitaire has caused a sensation among professional economists.

The theory has been worked out in its beginnings by Dr. John von Neumann, professor of mathematics at the Institute for Advanced Study, Princeton, N.J., and Dr. Oskar Morgenstern, professor of economics at Princeton University. In its present form the theory represents fifteen years of research, apart from the years spent by Dr. von Neumann before 1928 in working out the basic theory of games.

Dr. von Neumann, a collaborator of Albert Einstein, who did mathematical work important in the development of the atomic bomb, is recognized by his colleagues as one of the great original workers of the day in mathematics. He is the author of *Mathematical Foundations of Quantum Mechanics*. Dr. Morgenstern, former director of the Austrian Institute for Business Cycle Research at the University of Vienna, is considered one of the world's leading mathematical economists. He is the author of *Economic Forecasting*.

They published the results of their years of research in a 625-page book, *Theory of Games and Economic Behavior*, with nearly every page studded with formulae, mainly in the theory of sets and groups and in linear geometry. The book was issued by the Princeton University Press in September 1944.

Because the book was so "formidable" intellectually, as one professional critic put it, involving, as the authors admitted, "mathematical deductions" that "are frequently intricate," with "the logical possibilities" extensively exploited, the work went unnoticed for nearly a year and a half by the technical economic journals, with the exception of *The Annals of the American Academy of Political and Social Science*.

The current issue of *The American Economic Review*, journal of the American Economic Association, devotes a full-length article to the book, hailing it as "indeed a rare event," and the critics of other professional journals have pronounced the work an outstanding contribution.

Big Potentialities Seen

Prof. Leonid Hurwicz of Iowa State College, now on leave to the Cowles Commission for Research in Economics at the University of Chicago, writes in *The American Economic Review* that "the potentialities of von Neumann's and Morgenstern's new approach seem tremendous and may, one hopes, lead to the revamping and enriching in realism a good deal of economic theory."

Professor Hurwicz says "it would be doing the authors an injustice to say that theirs is a contribution to economics only."

"The scope of the book is much broader," he adds. "The techniques applied by the authors in tackling economic problems are of sufficient generality to be valid in political science, sociology, or even military strategy."

In mathematics as well as in economics the Neumann-Morgenstern approach represents a break with the traditional development. The mathematical theory of games was based on the calculus of probability. Thus it was concerned with the probable distribution of cards at any stage of the game.

It was shown, for example, that odds against any individual poker player's holding any of the forty classes of straight flushes before the draw are 64,973 to 1; that the drawing to two pairs, the chances are 11 to 1 against getting the third to either pair. In the 18th-century classic *Hoyle's Games*, the bible of the card and the horse player, many of these probability are given for card games and races, although the calculus then was in its infancy.

However, the present mathematical methods, essentially those of the differential and integral calculus, were not adequate for solving some of the problems of games. One unsolved problem, cited by Prof. E. J. Gumbel of the New School for Social Research, is that of a game with several participants, each trying to maximize his gain without being able to control the activity of other participants.

To solve these problems Professor von Neumann, in his preliminary work, "Zur Theorie der Gesellschaftspiele," published in *Annals of Mathematics* in 1928, and in the present work developed with Dr. Morgenstern a novel analytical apparatus drawn mostly from mathematical logic, set theory and functional analysis.

Strategies Analyzed

Using these new mathematical tools, they analyzed the strategies open to players in games of chance like dice-throwing and matching pennies and in games of

strategy like poker, bridge and chess. They proved that there might be no best strategy for a player to employ, or there might be several equally good ones.

In matching pennies, for example, where the opponent shakes up his pennies and lets them fall into an order fixed by chance, the best strategy is to adopt none. For Professors von Neumann and Morgenstern have proved that if the opponent "stacks" his pennies according to any preconceived plan, one can win by matching chance against strategy; that is, by shaking up the pennies and letting chance determine their order.

In chess, however, he proved that a good strategy existed because this is a game of perfect information, each player knowing at every stage of the game all the moves made previously.

Similarly for games of mixed strategies, where information is imperfect, they proved that a good strategy was possible. Each game, they showed, has its own characteristic function. Thus, as Louis Weisner of Hunter College has pointed out, for games of more than two players like poker, where the players may form coalitions that are decisive to strategies, "all questions relating to coalitions such as the forces which impel the formation of coalitions, the desertion of some members of a coalition to another, mergers or fights between coalitions, the division of profits or losses among members of a coalition are answerable in terms of the characteristic function."

Practical Use in Games

The solutions are too technical for brief exposition and cannot be given here. A brief exposition of a few takes seventeen pages in *The American Economic Review*. They will not be of practical use in games of chance and strategy, however, to experts in higher mathematics.

How Drs. von Neumann and Morgenstern discovered that the theory of games of chance could be used to analyze economic situations is not reported in their book. In a letter to this writer while the book was in preparation, Dr. Morgenstern explained that in carrying on his work in mathematical economics, he encountered many problems that could not be handled by the traditional tools drawn from the calculus, and hence he reached the conclusion that economics was following a blind alley in depending mainly on them.

They explain in the book, however, that they are not making a mere analogy between games and economics but seek to establish "that the typical problems

of economic behavior become strictly identical with the mathematical notions of suitable games of strategy." Their aim is the development of a theory that is mathematically rigorous and conceptually general, so that the science can go on, as all sciences have gone on, to genuine prediction by theory.

Five-sixths of the book is devoted to the mathematical theory, one-sixth to the economic applications. Among the latter are situations characterized by duopolistic and oligopolistic competition, where the market is dominated by two or a few sellers; the formation of coalitions, where buyers or sellers combine against other groups of buyers or sellers; and by organization of cartels. Not only "rational" but "irrational" economic behavior is comprehended by the theory.

Professor Hurwicz holds that reading the book will be a new stage in their education for the great majority of economists; the others may not be able to follow it.

Reader's Views Seen Affected

He says that because the non-economic results are more specific, mathematical readers "interested in the nature of determinacy of chess, in the theory of 'bluffing' in poker, or in the proper strategy for Sherlock Holmes in his famous encounter with Professor Moriarty" will enjoy the sections on strategic games proper. He adds, "the reader's views on optimum military or diplomatic strategies are also likely to be affected."

One defect of the theory is that it applies to capitalist economics only. This was pointed out by Mr. Gumbel in *The Annals*, and by Mr. Weisner in *Science and Society*. This criticism applies to the economic interpretation in terms of marginal utility economics, however, and not to the mathematics, the foundations of which Mr. Weisner found "firmly laid," arousing his admiration.

In sociological circles opinion was divided. The reviewer of the *American Journal of Sociology* "found the 'Theory of Games' at all times a model of clear and careful exposition." The reviewer in *Social Forces* reported "this may be an extremely valuable new direction or it may be an interesting but useless development." While very few problems of a strictly sociological nature were attempted, Drs. von Neumann and Morgenstern believe that sociometric problems are best approached from this direction.

March 10, 1946

Soap Bubbles Get a New Role in Old Mathematics Problem

By JOSEPH WILLIAMS

“A soap bubble,” Mark Twain mused in a passage of *The Innocents Abroad*, “is the most beautiful thing, and the most exquisite, in nature . . . I wonder how much it would take to buy a soap bubble if there was only one in the world?”

Fortunately for theoretical mathematicians, it is no problem to make any number of soap bubbles, the iridescent fragile spheres that are being used to tackle the descendants of an old, yet still intriguing problem: If you have a given closed three-dimensional curve, what is the surface of smallest area bounded by that curve?

This problem, which defied any solution until 1930, fascinated Joseph A. F. Plateau, a Belgian physicist, who did research involving many of the laws governing the behavior of soap films and bubbles.

Since then, the challenge has been taken up by a number of pure mathematicians, including Frank Morgan, who began studying the mathematics of soap films and bubbles several years ago as a graduate student at Princeton University.

Research Is Augmented

Now, as an assistant professor at the Massachusetts Institute of Technology, Dr. Morgan has continued his research, which recently led to a major finding. He augments his studies by experiments with easy-to-bend wire and several gallons of his four-year-old soap film brew, a mixture of one part water, one part dish-washing detergent and, to aid the films' stability, some glycerin.

The roots of “Plateau's problem” lie in early research on the calculus of variations, a discipline that involves solving problems on the smallest and largest values of quantities, such as the area of surfaces. These problems are encountered in many fields, such as business and physics.

Soap films, Dr. Morgan said in a telephone interview, provide a “rather direct and simple way” to look at these maximum and minimum problems.

In the real world, a twisted wire is analogous to the mathematical curve. After the wire is dipped into and pulled out of a soap solution, the resulting soap film or cluster of soap bubbles tries to reduce its surface tension, or surface energy,

by forming a geometric shape with the least possible area. This "area-minimizing effect" is easily demonstrated in the case of a very simple curve, such as a flat circular frame, for which the surface of least area is a flat disk.

When Results Are Paired

The same rules apply with soap bubbles, which represent the surfaces of least area enclosing a quantity of air. When two bubbles join, for instance, there is a pair of results: the surface area of the bubble cluster is less than the combined surface areas of the original bubbles, and a third surface is formed.

Regardless of the bubbles' sizes, it has been found, several geometric laws are constant. When three surfaces meet on a curve, angles of 120 degrees are always formed, and angles of about 109 degrees result when four such curves meet at a point.

In the early 1900s, the shapes considered to be answers to Plateau's problem were relatively simple. Most were attained by bending and stretching a circular disk. Conceptual advances since 1930 have allowed studying a wide array of shapes with unlimited complexity, including one proposed in 1950 by the mathematician Richard Courant.

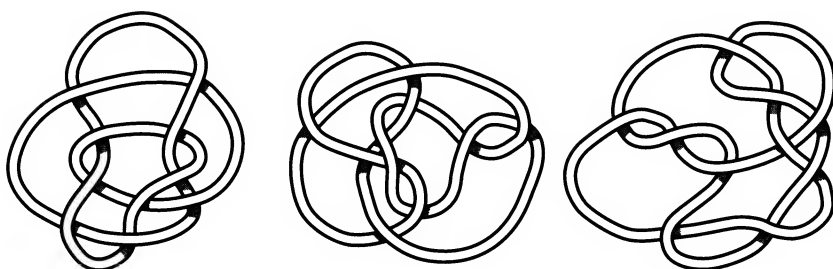
Mathematicians were well aware at the time that a few wire shapes were known to bound two or more different soap films. Then Courant came up with a wire shape that bounded an infinite number of different soap films.

This curve solved one problem, but created others, because it was badly twisted and at one spot it headed in infinite directions. Dr. Morgan recently found a smooth shape that satisfies the conditions of the problem. Still, he reports one disappointment: The infinite number of different soap films are unstable and will probably never be observed in nature or in the laboratory.

October 17, 1982

Math Advance Penetrates Secrets of Knots

By JAMES GLEICK



A series of surprising discoveries is helping the practitioners of one of the purest forms of mathematics, the theory of knots, to attack a fundamental problem of their discipline: how to distinguish one knot from another.

At the same time, the advances are providing a new kind of tool for scientists studying twisting, looping stringlike structures in chemistry and molecular biology. Among other things, the mathematical understanding of knots seems to hold direct promise for scientists deciphering the way strands of molecules organize themselves into the complex structures of DNA.

A theorist's knot is a formalized, standardized, idealized version of the everyday object—a closed loop of one-dimensional string that winds through three-dimensional space. It is one of the quintessential shapes that nature can take in the mind of a mathematician. Problems of naming, classifying and understanding knots have proved extremely hard.

Pictures of DNA clearly show knots, with turns and crossings made visible by a new process of coating the molecules to prepare them for the electron microscope. The mathematical discoveries seem to provide a key to the way one structure changes to another in life's basic processes of replication and recombination.

"This is a very unusual joining of mathematics and biology," said Kiyoshi Mizuuchi of the National Institutes of Health. "You can gain very strong information about enzymes that is otherwise impossible to gain."

Above all, chemists and molecular biologists are realizing that important features can be understood by adopting the knot theorist's view of reality. Where Euclidean geometry thinks of structures as rigid, a knot theorist thinks in terms of complete flexibility. That is the essence of topology, the "rubber-sheet geometry"

of which knot theory is one branch. Distances and measurements are irrelevant. If a certain knot can be bent, twisted, stretched, squeezed or otherwise deformed into another knot—without being cut or untied—then the two are equivalent.

The most basic topological principles can be difficult to prove. For example, deciding whether two knots, drawn on paper or modeled in string, are the same or different turns out to be a penetrating puzzle. The outline of the problem is familiar to anyone who has ever untied a package or unknotted a skein of yarn, but its essence has occupied mathematicians for nearly a century and now seems closer than ever to the heart of modern geometry.

"There are lot of hidden difficulties in the subject," said Morwen B. Thistlethwaite, a mathematician at Polytechnic of the South Bank in London. "The problems are easy to state but quite difficult to solve. And the techniques have become very high-powered."

Indeed, the great issues in knot theory sometimes surface in the guise of recreational brain-teasers. For example, suppose "cheating" is defined as passing one part of a closed knot through another part. How many times do you have to cheat to turn a given knot into the "unknot," or circle? For one knot that can be drawn with just eight crossings, the answer has only recently been shown to be two, with the proof requiring 300 pages of dense analysis. For other simple knots, the unknotting number remains unknown.

Certainty Is Elusive

A running theme of such problems is that a solution may seem obvious up to all but the very last degree of certainty. Cheating once may seem inadequate to unknot. Two knots may seem different, and after hours of untwisting and unlooping you may feel sure—experimentally. But perhaps you have just not been patient or clever enough. Neither the eye nor the hand can tell for sure. A mathematician needs a system.

Where a sailor classifies knots in terms of physical characteristics, a mathematician needs a well-defined way of listing patterns of loops and crossings. As knots get more complicated, the complexities multiply. The simplest possible knot, known as the trefoil, is drawn with just three crossings. It is unique, save for its mirror image. Similarly, there is just one knot with four crossings, and just two with five. But 165 distinct knots have 10 crossings, and the total through 13 crossings—the highest number for which a complete catalogue now exists—is 12,965 knots.

Since the first great catalogings of knots in the 19th-century by the Scottish physicist Peter Guthrie Tait and the American mathematician C. N. Little, mathematicians have tried searching for "invariants," or fundamental properties that tell one knot from another. The perfect invariant would distinguish any pair of knots. Short of perfection, some invariants do better than others.

The newest breakthrough in knot theory has been the discovery of invariants of a particularly powerful kind, capable of distinguishing knots where other invariants failed. Several groups of mathematicians independently worked out sets of rules that would let them take any knot and systematically turn it into an algebraic expression known as a polynomial, a combination of numbers and variables.

The polynomial serves as a kind of label for the knot. Unlike the knots themselves, the polynomials can be told apart just by looking. And if the polynomials for two knots are different, then the knots are different; unfortunately, if they are the same, the knots may or may not be the same.

Size and Shape Irrelevant

As in all topological problems, the particular size or shape of a loop is irrelevant. All that matter are the direction of the crossings, over or under, and their arrangement in relation to the other crossings.

The first polynomial invariant, and until recently the only one, was discovered in the 1920s. It distinguished many knots, but mathematicians could not predict when it would work and when it would not.

In 1984, Vaughan F. R. Jones of the University of California at Berkeley—an expert not in knot theory but in algebra—discovered a new polynomial invariant, and since then a succession of other mathematicians have taken his discovery further.

"It's a very exciting, astonishing development," said Joan S. Birman, a Barnard mathematician who is an authority on knots and their near-relations, braids. "It's important for knot theory and it's important in a bigger sense because it's a bridge between two very different areas of mathematics, where people never imagined there was a connection."

Three hundred mathematicians from a variety of fields—and some molecular biologists as well—will discuss the new developments at a conference beginning next week in Santa Cruz, Calif.

"It's opened up a whole vista on a part of mathematics that wasn't even guessed at before," said David Yetter of Clark University in Worcester, Mass. He and five other mathematicians discovered another new polynomial informally known as the Homfly, from the initials of their surnames. "It's symptomatic of something that's happening now to mathematics as a whole—fields being discovered to be interrelated when everybody thought they had been developing separately," Dr. Yetter said. "They're all starting to constellate and become part of some whole."

As powerful as the new techniques are, they are also tantalizingly enigmatic: so far, knot theorists cannot quite explain why they work as well as they do. Somehow, the process of turning a physical structure into an abstract algebraic expression must capture some essence of the knot, but no one knows exactly what. In a sense, the mathematicians understand the algebra behind the new discoveries, but not the geometry.

"They're magic," Dr. Birman said. "It's magic that we're doing. This polynomial catches hold of something, but it's terribly hard to say what it is."

Without the new invariants it was possible to classify all knots up to 13 crossings, a task completed in 1982, but the process was arduous and error-prone. Even proving the trefoil to be different from the unknot was hard, and using earlier methods to distinguish two difficult knots could require enormous computation. In theory, it might require millions of hours of computing time. The new polynomials are much faster.

"They're simultaneously extremely important and infuriatingly simple," said Jonathan Simon, a University of Iowa mathematician. "People should have seen these earlier—'people' meaning all knot theorists for the last 20 years."

Dr. Simon is one of several mathematicians who have gone beyond the usual boundaries of their customarily abstract discipline to begin exploring the implications for chemistry.

Chemists have known for years that molecules can take the form of knots, and other structures as well: linked rings, or "catenanes," for example. But until recently most geometrically minded chemists thought in terms of rigid models, rather than infinitely flexible ones.

"Now chemists have begun making molecules where the difference in how they sit in space is due to topology, not rigid geometry," Dr. Simon said. "Topology is chock full of beautiful pictures and neat ideas, and there's some fascination with just the ideas and pictures, but here also is real substance."

Other chemists and biologists are studying the peculiar waves that propagate through certain chemical reactions or arrays of muscle cells. In such "excitable media," a stimulus produces a reaction that spreads from place to place like a wave rippling outward in a pond. The sheet of nerve cells in the retina is one example, and the heart muscle is another. In three dimensions, such waves can take fantastic shapes, and the cores of these shapes can form threadlike filaments.

"Pieces of Spaghetti"

"When you have a spatially extended medium you can have structures, threads, pieces of spaghetti," said Arthur T. Winfree, a theoretical biologist who has done extensive simulation of excitable media in the laboratory and with powerful computers. "All this mathematics can be picked up lock, stock and barrel and used in an entirely different context."

The filaments, as it happens, can be linked or even knotted. And distinctive topological shapes seem to produce distinctive kinds of behavior.

In molecular biology, the most famous three-dimensional structure is DNA, with its supercoiled double helix joining two strands and compressing their genetic information into a manageable region of space. The supercoiling—coiling of coils—stores energy that cells can use, like the energy in a twisted rubber band.

The coiling also creates a formidable topological problem when the strands need to pull apart and rejoin in the process of recombination. Biologists investigating such processes have changed their emphasis. Instead of concentrating exclusively on the arrangement of DNA's building blocks, base pairs, as though the strands were simply straight lines, many biologists are focusing more and more on the flexible arrangements of the strands in space.

"We've Had A Field Day"

Often the structures seem to affect the workings of enzymes, which serve as agents and messengers in the recombination process. "This is where we've had a field day, where there has been the prettiest combination of mathematics and biochemistry," said Nicholas R. Cozzarelli, a molecular biologist at the University of California at Berkeley who pioneered the coating technique that made DNA knot pictures possible.

Knot theory now enables biologists to look at beginning and ending stages of an enzyme reaction and deduce what the middle stages must have been. It also lets them predict the possible ways in which enzymes temporarily break strands to allow unknotting. The new Jones polynomial, in particular, seems to provide a way of quantifying such processes, perhaps because it is especially sensitive to crossings in knots.

For most mathematicians, the chemical and biological applications remain a side issue—nice to know, but not especially surprising. The future of knot theory, as they see it, will be what the past has been, the study of a special kind of intricacy, for its own sake.

July 8, 1986

Packing Tetrahedrons, and Closing in on a Perfect Fit

By KENNETH CHANG

More than 2,300 years ago, Aristotle was wrong.

Now, in the past year, a flurry of academic activity is suddenly zooming in on an answer to a problem akin to wondering how many people can fit into a Volkswagen Beetle or a phone booth. Except here mathematicians have been thinking not about the packing of people, but of geometric solids known as tetrahedrons.

"It's pretty remarkable how many papers have been written on this in the past year," said Henry Cohn, a mathematician at Microsoft Research New England.

A tetrahedron is a simple construct—four sides, each a triangle. For the packing problem, researchers are looking at so-called regular tetrahedrons, where each side is an identical equilateral triangle. Players of *Dungeons & Dragons* recognize the triangular pyramid shape as that of some dice used in the game.

Aristotle mistakenly thought that identical regular tetrahedrons packed together perfectly, as identical cubes do, leaving no gaps in between and filling 100 percent of the available space. They do not, and 1,800 years passed before someone pointed out that he was wrong. Even after that, the packing of tetrahedrons garnered little interest. More centuries passed.

A similar conundrum for how to best pack identical spheres has a more storied history. There, the answer was obvious. They should be stacked like oranges at a supermarket (with a packing density of 74 percent), and that is what Johannes Kepler conjectured in 1611. But proving the obvious took almost four centuries until Thomas C. Hales, a mathematician at the University of Pittsburgh, succeeded in 1998 with the help of a computer.

With tetrahedrons, the best packing arrangement is not obvious, and after it was pointed out that tetrahedrons did not pack perfectly, it seemed that they did not pack very well at all. In 2006, two Princeton University researchers, Salvatore Torquato, a chemist, and John H. Conway, a mathematician, reported that the best packing they could find filled less than 72 percent of the space—packing more loosely than spheres. That ran counter to a mathematical conjecture that, among so-called convex objects (those without dimples, holes or hollows), spheres should have the loosest ideal packing.

The Princeton paper prompted Paul M. Chaikin, a professor of physics at New York University, to buy tetrahedral dice by the hundreds and have a high school student stuff them into fish bowls and other containers. "We immediately found you could do better than 72 percent," said Dr. Chaikin, who had earlier worked with Dr. Torquato on the packing of squashed spheres, or ellipsoids. (It turned out that squashed spheres pack more densely than spheres.)

The Princeton paper also led Jeffrey C. Lagarias, a mathematics professor at the University of Michigan, to ask Elizabeth Chen, one of his graduate students, to look at tetrahedron packing. Ms. Chen recalled his telling her: "You've got to beat them. If you can beat them, it'll be very good for you."

Ms. Chen examined several hundred arrangements over the next few weeks, and, she said, "there happened to be several that stood out as very dense." Her best packing easily eclipsed what Dr. Conway and Dr. Torquato had found, with a packing density of almost 78 percent, surpassing spheres.

"In fact, my adviser totally did not believe me," Ms. Chen recalled.

After making physical models of tetrahedrons and demonstrating the packing patterns, she convinced Dr. Lagarias that her packings were as dense as she had said they were, and finally published her findings a year ago.

Meanwhile, Sharon C. Glotzer, a professor of chemical engineering also at the University of Michigan, was interested to see whether the tetrahedrons might line up as liquid crystals do. "We got into it, because we are trying to design new materials for the Air Force that have interesting optical properties," she said.

Dr. Glotzer and her colleagues wrote a computer program that simulated the jostling of tetrahedrons and how they arranged themselves when pushed together. They found not liquid crystals but complex quasicrystal structures with patterns almost repeated yet not quite. "That is the most astonishing crazy thing," Dr. Glotzer said.

Examining the quasicrystals, they did find a periodic structure that represented another leap in packing density: over 85 percent. Just as that finding was prepared for publication last month in the journal *Nature*, a group at Cornell, using a different search method, found yet another packing that was just as dense.

But while Dr. Glotzer's structure was surprisingly complex—the repeat pattern consists of 82 tetrahedrons—the Cornell crystal was surprisingly simple, with just four. It is also puzzling to researchers why the tetrahedrons in Dr. Glotzer's simulations tend to the complex quasicrystal structures if the best packing is actually a much simpler structure.

"That's part of what's so surprising about this," said Dr. Cohn, of Microsoft Research. "Each of these packings feels very different."

A few days before Christmas, Dr. Torquato and Yang Jiao, a graduate student, reported that they had tweaked the Cornell structure to bump up the packing density by a fraction, to 85.55 percent.

"I'd be shocked if what we have right now is the densest," Dr. Torquato said in an interview last week. "It just happens to be the densest known right now."

Dr. Torquato need not be shocked.

On Monday, Ms. Chen, the University of Michigan graduate student, posted a new preprint, which describes a family of packings that include the latest Cornell and Princeton structures. But it also includes a better packing. The calculation was verified by simulations from Dr. Glotzer's group.

The new world record for packing density of tetrahedrons: 85.63 percent.

January 4, 2010

Finding Order in the Apparent Chaos of Currents

By BINA VENKATARAMAN

Suppose a blob of dioxin-rich pesticide is spilled into Monterey Bay. It might quickly disperse to the Pacific Ocean. But hours later, a spill of the same size at the same spot could circle near the coastline, posing a greater danger to marine life. The briny surface waters of the bay churn so chaotically that a slight shift in the place or time an oil drop, a buoy—or even a person—falls in can dictate whether it is swept out to the open ocean or swirls near the shore.

But the results are not unpredictable. A team of scientists studying Monterey Bay since 2000 has found that underlying its complex, seemingly jumbled currents is a structure that guides the dispersal patterns, a structure that changes over time.

With the aid of high-frequency radar that tracks the speed and direction of the flowing waters, and computers that rapidly perform millions of calculations, the scientists found that a hidden skeleton guided whether floating debris lingered or exited the bay.

Over the past 10 years, scientists have made enormous strides in their ability to identify and make images of the underlying mechanics of flowing air and water, and to predict how objects move through these flows.

Assisted by instruments that can track in fine detail how parcels of fluid move, and by low-cost computers that can crunch vast amounts of data quickly, researchers have found hidden structures beyond Monterey Bay, structures that explain why aircraft meet unexpected turbulence, why the air flow around a car causes drag and how blood pumps from the heart's ventricles. In December, the journal *Chaos* will highlight the research under way to track the moving skeletons embedded in complex flows, known as Lagrangian coherent structures.

"There's been an explosion of interest in this area," said David K. Campbell, editor in chief of *Chaos*, a physicist and provost at Boston University. "Why it's become more interesting is that experimentalists can now watch these structures emerge."

The patterns of flow have fascinated thinkers for centuries. In the 1500s, Leonardo da Vinci sketched the swirling eddies he saw in rivers and the vortexes

of blood he imagined in the aortic valve. Just as those visible patterns of flow change quickly, eluding our ability to predict the fate of objects caught up in them, the hidden structures of flow also move and morph over time.

The concept of the structures grew out of dynamical systems theory, a branch of mathematics used to understand complicated phenomena that change over time. The discovery of the structures in a wide range of real-world cases has shown that they play a key role in complex and chaotic fluid flows in the atmosphere and ocean.

The structures are invisible because they often exist only as dividing lines between parts of a flow that are moving at different speeds and in different directions. In the ocean, the path of a drop of water on one side of such a structure might diverge from the path of a drop of water on the other side; they will drift farther apart as time passes.

"They aren't something you can walk up to and touch," Jerrold E. Marsden, an engineering and mathematics professor at Caltech, said of the structures. "But they are not purely mathematical constructions, either."

As an analogy, Dr. Marsden suggests imagining a line that divides a part of a city that has been affected by a disease outbreak from a part that has not. The line is not a fence or a road, but it still marks a physical barrier. And as the outbreak spreads, the line will change.

To find the structures, scientists must track flow, not by watching it go by but from the perspective of the droplets of water or molecules of air moving in it. "It's like being a surfer," Dr. Campbell said. "You want to catch the wave and move with the wave."

In the laboratory, researchers shine lasers on tiny particles caught in a flow, capturing their speed and trajectory with fast, high-resolution digital cameras similar to the way tracer rounds from machine guns track the path of bullets. In the ocean or atmosphere, scientists rely on instantaneous data from high-frequency radar, laser detection systems, buoys and satellites. In the human body, phase-contrast magnetic resonance imaging has helped researchers map the complex patterns of blood flow in detail. Computers take in the data from all those sources, applying algorithms that unveil the flow structures.

"We're just recognizing that these things exist and are playing a role in a variety of scenarios," said Thomas Peacock, a mechanical engineering professor at M.I.T. who is evaluating how Lagrangian coherent structures affect vehicle performance and efficiency. "The idea is that cars, airplanes and submarines down

the line would be fitted with sensors that will help them adapt to these structures.”

Studies of the air flow patterns surrounding Hong Kong International Airport have shown that Lagrangian coherent structures cause unexpected jolts to planes during landing attempts, forcing pilots to waste fuel while they revert to holding patterns. George Haller, an engineering professor at McGill University in Montreal who forged the mathematical criteria for finding such structures in fluid flows, is working with the airport’s officials to design a tool that allows pilots to see and navigate around the structures. It will rely on data from laser scans, analyzed by computers as planes approach the airport.

At Stanford, researchers are mapping blood flow in patients with abdominal aortic aneurysms to see whether frequent exercise changes the flow structures in ways that correlate to slower bulging of the artery.

The scientists studying Monterey Bay found a Lagrangian coherent structure that acts as a moving ridge, separating a region of the bay that spreads pollutants out to sea and a region that recirculates them in the bay. They watched this ridge drift and change over 22 days and found that if computed in real time, it could be used to predict one-day windows when pollutants could do less damage to the bay environment.

The scientists proposed building a holding tank for the fertilizers and pesticides that wash from farmland into the neighboring watershed that could release pollutants only at times when they would quickly drift into the ocean, where they would be so diluted they would pose less harm to marine life. In a later experiment, scientists found that the path of buoys dispatched in the bay followed the path predicted by the computer simulations.

Researchers who studied the waters along the southeastern coast of Florida found a similar structure that they argued could be used to reduce the effects of pollution near Hollywood Beach, south of Fort Lauderdale.

Their research in Monterey Bay piqued the interest of Art Allen, a physical oceanographer for the Coast Guard who thinks that Lagrangian coherent structures could improve search-and-rescue operations for people lost at sea by offering more precision than current techniques.

Researchers in private industry and the French Navy have expressed interest in using models of the structures to track the spread of oil after spills in coastal areas, said Francois Lekien, an applied mathematics professor at the École Polytechnique at the Université Libre de Bruxelles in Belgium who was a co-author of the bay studies.

Strategies based on Lagrangian coherent structures have yet to be tested to see if they curb coastal pollution. And they have several limitations. Scientists cannot yet predict what happens to pollutants that do not float on the ocean surface. The models do not yet account for the interaction with wind patterns that also guide how floating objects or people drift at sea. The method also requires continuing, detailed data akin to what was available in Monterey Bay, which has an ocean monitoring program that far surpasses that of most coastal areas.

Even if the structures in flow do not guide engineering or pollution strategies as well as researchers hope, many scientists believe that unearthing and visualizing them provides useful insights. For example, the structures identified in coastal waters have exposed flaws in our intuition about flow. "There are myths out there that it's O.K. to dump pollutants at high tide," said Dr. Marsden, co-author of the Monterey Bay and coastal Florida studies. "But it's really these structures that will determine where pollutants end up."

Finding the structures in various settings has also given researchers a fresh perspective on what remains a great scientific puzzle: the dynamics of flow.

"In complex systems such as the atmosphere, there are a lot of things that people can't explain offhand," Dr. Haller said. "People used to attribute this to randomness or chaos. But it turns out, when you look at data sets and find these structures, you can actually explain those patterns."

September 28, 2009

In Bubbles and Metal, the Art of Shape-Shifting

By KENNETH CHANG



The next time you stare into a beer, contemplate the bubbles.

Mathematicians and scientists do. But for the thousands of years that brewers have been brewing beer, those beer-drinking researchers have not had an equation to describe how the bubbles change over time.

Now they do.

David J. Srolovitz, a professor of physics at Yeshiva University in Manhattan, and Robert D. MacPherson, a mathematician at the Institute for Advanced Study in Princeton, N.J., reported the solution last month in an article in the journal *Nature*.

Anheuser-Busch and Guinness may not have noticed, but that was not the point. "At the end of the day, I don't think it's going to revolutionize beer making," Dr. Srolovitz said. "This is mathematics."

Of more practical use, the equation also applies to metals. A piece of steel or aluminum might look like one uniform piece, but it consists of a conglomeration of many tiny crystalline grains, and the strength and flexibility of a metal depend largely on the size, shape and orientation of the grains.

That has been known, intuitively, at least, as long as there have been blacksmiths. The smiths' "heat and beat" technique, in addition to bending metal to the desired shape, alters the grains and properties of the metal.

When heated, atoms jump from the surface of one grain to a neighboring one. Some grains grow, and some shrink. "This grain-growth process is what happens when you anneal and hold it at different times and different temperatures," Dr. Srolovitz said.

In beer bubbles, air diffuses from one bubble to the next, and the bubbles change size and shape. The two processes—growth of bubbles and metal grains—are mathematically almost identical.

Foundries today are bigger and more complex, but the underlying knowledge remains based more on experience rather than science. Even when material

scientists know of a desirable arrangement of metal grains, they have to discover by experiment a process that can produce it.

"It's completely trial and error," said David Kinderlehrer, a professor of mathematics at Carnegie Mellon who wrote an accompanying commentary in *Nature*.

More than half a century ago, John von Neumann, mathematician and computer science pioneer, solved the two-dimensional version of the problem almost as a passing comment on someone else's scientific paper. "It was intuitively obvious to him," Dr. Srolovitz said.

The problem in three dimensions, however, eluded solution. Dr. Srolovitz and Dr. MacPherson started their work after Dr. MacPherson, who was looking to apply his mathematical knowledge to science, sat in on one of Dr. Srolovitz's classes at Princeton, where Dr. Srolovitz was a professor before moving to Yeshiva last year.

Their solution is surprisingly simple. A boundary between two grains or bubbles moves at a velocity proportional to the boundary's curvature. "This equation will basically tell you the relationship between time and grain size," Dr. Srolovitz said.

That, in turn, could aid in engineering novel materials like shrink-wrap steel or less corrosive batteries, Dr. Kinderlehrer said. "This is really a signature achievement. The result is so simple you can use it."

Materials scientists will still have to add other complications to their computer simulations like the effects of impurities.

It also does not provide a full solution to the beer foam, because it does not account for effects like gravity, which pulls liquid down the beer bubble walls until the walls are too thin and bubbles pop.

On the other hand, Dr. Srolovitz and Dr. MacPherson's equation works not only for three dimensions, but all possible dimensions. That could be useful for someone wanting to contemplate, for instance, what happens to a 67-dimensional beer.

May 22, 2007

The Scientific Promise of Perfect Symmetry

By KENNETH CHANG

It is one of the most symmetrical mathematical structures in the universe. It may underlie the Theory of Everything that physicists seek to describe the universe.

Eighteen mathematicians spent four years and 77 hours of supercomputer computation to describe this structure, with the results unveiled Monday at a talk at the Massachusetts Institute of Technology.

But it still is not easy to describe the description, at least not in words.

"It's pretty abstract," conceded Jeffrey D. Adams, a professor of mathematics at the University of Maryland who led the project.

For mathematicians and physicists, symmetry can provide crucial insights into a problem. A 19th-century Norwegian mathematician, Sophus Lie (rhymes with tree), wrote down what are now known as Lie groups, sets of continuous transformations—meaning the changes could be a little or a lot—that leave an object unchanged in appearance.

For example, rotate a sphere any distance around any axis, and the sphere looks exactly the same.

Later mathematicians found five exceptions to the four classes of Lie groups that Lie knew about. The most complicated of the "exceptional simple Lie groups" is E8. It describes the symmetries of a 57-dimensional object that can in essence be rotated in 248 ways without changing its appearance.

Why are there five exceptional Lie groups? "It's just one of the beautiful magical things that happen in mathematics," Dr. Adams said.

"You can't really picture it," Brian Conrey, executive director of the American Institute of Mathematics, said of E8. The institute sponsored the project with financing from the National Science Foundation.

"It's some sort of curvy, torus type of thing," Dr. Conrey said. "Now you start to move it around in different ways. It's an amazingly symmetric group."

To understand using E8 in all its possibilities requires calculation of 200 billion numbers. That is what Dr. Adams's team did, a rare collaboration for mathematicians who usually work alone or in small groups and rarely turn to supercomputers.

Robert L. Bryant, a mathematician at Duke who was not involved in the project, gave a biological analogy. Scientists can learn a lot about an animal from its DNA, but to understand it fully “you have to grow the organism and then study it,” Dr. Bryant said. “In a certain sense, that is what the E8 team did. They used massive computation to fully develop the group E8 and its representations so that they could list its important features.”

One eventual use could be understanding the universe, another example of physics taking advantage of abstract math. Isaac Newton invented calculus to study the motion of objects. Fourier analysis, the mathematics of periodic patterns, proved essential in studying phenomena like light waves, and physicists have employed Lie groups in quantum mechanics and relativity.

“All of the physics of the 20th century is tied up with this language,” Dr. Conrey said.

E8 is the Lie group underlying some superstring theories that physicists are pursuing in an effort to tie gravity and the other fundamental forces of the universe into one theory.

“It could well be E8 that determines the deep inner structure of the universe,” Dr. Adams said.

March 20, 2007

143-Year-Old Problem Still Has Mathematicians Guessing

By BRUCE SCHECHTER

In the early years of the 20th century, the great British mathematician Godfrey Harold Hardy used to take out a peculiar form of travel insurance before boarding a boat to cross the North Sea. If the weather looked threatening he would send a postcard on which he announced the solution of the Riemann hypothesis. Hardy, wrote his biographer, Constance Reid, was convinced "that God—with whom he waged a very personal war—would not let Hardy die with such glory."

The Riemann hypothesis, first tossed off by Bernhard Riemann in 1859 in a paper about the distribution of prime numbers, is still widely considered to be one of the greatest unsolved problems in mathematics, sure to wreath its conqueror with glory—and, incidentally, lots of cash. Two years ago, to celebrate the millennium, the Clay Mathematics Institute announced an award of a million dollars for a proof (or refutation) of the hypothesis.

Whether in pursuit of glory, cash ("prizes attract cranks," one mathematician sniffed) or pure mental satisfaction, more than a hundred of the world's leading mathematicians came to New York City recently to attend an unusual conference at New York University's Courant Institute. While most math conferences are devoted to presenting completed work, this one was held for mathematicians to swap hunches, warn of dead ends and get new ideas that could ultimately lead to a solution.

"One of the things we hope to do is to consolidate the approaches," said Dr. Brian Conrey, a professor of mathematics at Oklahoma State University and executive director of the American Institute of Mathematics, a private group that organized the meeting with support from the Courant Institute and the National Science Foundation. "We're looking for brand-new ideas with which to open the door."

There was a guarded optimism among the mathematicians that promising new ideas were being put forward, but in mathematics prognostication is a dangerous game. Hardy, for example, rated the Riemann hypothesis less difficult than Fermat's conjecture, which Dr. Andrew Wiles of Princeton solved in 1993, after working for seven years in secrecy. Dr. Wiles, as it happens, dropped in on the conference, but when asked if this meant he was now attacking the hypothesis he shrugged and said, "Well, it's a spectator sport, you know."

As in all sports, it helps to know the rules of the game. Riemann made his hypothesis in the course of a 10-page paper he wrote on the distribution of prime numbers that is considered to be one of the most important papers in the history of number theory, a history that stretches back more than 2,500 years.

Prime numbers are numbers that are divisible only by one and themselves—they are the atoms of arithmetic, for any number is either a prime or a product of primes. The first few primes are 2, 3, 5, 7, 11 and 13—but despite their simple definition the prime numbers appear to be scattered randomly amid the integers.

There is no simple way to tell if a number is prime, and that is the basis for most modern encryption schemes. Solving the hypothesis could lead to new encryption schemes and possibly provide tools that would make existing schemes, which depend on the properties of prime numbers, more vulnerable.

Despite the random occurrence of individual primes, the primes themselves were found to follow a remarkably simple distribution. In 1792, when he was 15, Karl Friedrich Gauss decided to examine the number of primes less than a given number. He discovered that the primes became, on average, sparser the further out he looked and that this dwindling obeyed a simple, logarithmic law. He had no idea why this was so, but it was intriguing.

In 1859, Riemann, who had been a student of Gauss, took up the question of the distribution of primes in his only paper on number theory. With that paper he revolutionized the field, as he had the fields of geometry (his math became the basis for Einstein's theory of gravitation) and several other branches of mathematics. What Riemann discovered was a way of using the properties of a relatively simple function to count the primes.

What was so remarkable about Riemann's zeta function was that it somehow took a question about prime numbers—those discrete atoms of simple arithmetic, things easy to imagine—and put it in terms of a far larger and more esoteric class of numbers known as complex numbers. Complex numbers are a generalization of the familiar decimal numbers that mathematicians call the real numbers.

While the real numbers can be thought of as points on an infinite line, the complex numbers are points on a plane. One axis of this complex plane corresponds to the real numbers, and the other corresponds to the "imaginary" numbers—which were introduced so that negative numbers could have square roots, and are no more imaginary than real numbers. A function like Riemann's zeta function is simply a rule that takes a point on this plane and sends it to some other point.

By moving the problem to the complex plane Riemann had access to a whole new set of powerful mathematical tools, many of which he had developed himself. What was going on with the primes turned out to be a shadow of what was going on in this more general world.

Riemann showed that if he knew where the value of his zeta function went to zero he would be able to predict the distribution of the primes. He was able to prove that aside from some "trivial" zeros—located at -2 , -4 , -6 , and so on and thus easily included in his equations—the zeros of the zeta function all lay within a strip one unit wide running along the imaginary axis. •

Somehow the distribution of these zeros mirrored or encoded the distribution of the prime numbers. Riemann guessed that all of the zeros ran along the middle of the critical strip like the dotted line on a highway. Nobody is sure why he made this guess, but it has proven to be inspired. Over the past few decades billions of zeros of the zeta function have been calculated by computer, and every one of them obeys Riemann's hypothesis.

Most of the conference attendees would be shocked if a stray zero were found and Riemann was proven wrong. They would agree with John Fry, the chief executive of Fry's Electronics and a math major who used his fortune to found the mathematics institute. "I think we would have a better chance of finding life on Mars than finding a counterexample," he said.

But the field is rife with examples of hypotheses that seem to be true but are subsequently proven to fail at numbers beyond the reach of any conceivable computer. Only a mathematical proof, based on logic, can handle questions of the infinite.

Still, calculating the zeros of zeta is not an idle pursuit. In 1972, Hugh Montgomery, a mathematician at the University of Michigan, investigated the statistical distribution of the zeros. He found that they were scattered randomly but seemed to repel each other slightly—they did not clump together. On a trip to the Institute for Advanced Study in Princeton he showed his result to the physicist Freeman Dyson.

By sheer luck, Dr. Dyson was one of the few people in the world who would have recognized that the Montgomery results looked just like recent calculations on the energy levels of large atoms. The coincidence was so striking that it forged a new and still mysterious bridge between quantum physics and number theory. The connection was one of many pursued at the conference, though Dr. Montgomery does not think this work will lead directly to a solution. "It only gives us clues," he said.

Other clues abounded at the conference, some tantalizing, such as possible linkages to the theories Dr. Wiles developed to solve the Fermat conjecture. But mathematical proofs are extremely delicate structures that can dissolve at the merest touch.

Dr. Peter Sarnak, from the Institute for Advanced Study, spoke to the meeting about a promising approach that he and his colleagues have been pursuing. Just as Riemann attacked the problem of the primes by generalizing the zeta function to the complex plane, Dr. Sarnak and many others have been looking at families of functions of which Riemann's zeta function is just one relative. Each of these functions has its own Riemann hypothesis. "Of course," Dr. Sarnak acknowledged, "often the reason you generalize is that you're stuck."

But generalization also has its rewards. While the Riemann hypothesis does not have very many applications, the generalized version, if true, would solve hundreds of important mathematical problems.

When Dr. Wiles sat down in his attack to solve Fermat's conjecture, his path, though it would require genius to traverse, was clear: recent results had indicated the most promising direction to travel. Mathematicians at the conference agreed that there was no such clear evidence of a trail head for the Riemann hypothesis, a challenge they called both frustrating and exhilarating.

"The Riemann hypothesis is not the last word about things," Dr. Montgomery said. "It should be the first fundamental theorem. We're in a kind of logjam right now because we can't prove the fundamental theorem."

July 2, 2002

What Is the Most Important Problem in Math Today?

By GINA KOLATA

Many mathematicians would say it's the problem they're working on, but of all the famous unsolved problems, one stands out—the Riemann hypothesis. Posed in 1859 by the German mathematician Georg Friedrich Bernhard Riemann, it has tantalized mathematicians ever since. Recently, efforts to prove it have taken on a new intensity, with mathematicians turning to physics for insight.

The conjecture is Riemann's only venture into number theory, a branch of mathematics that investigates whole numbers. And it says something truly profound about prime numbers. Such numbers, like 2, 3, 5 and 7, have no divisors other than themselves and 1 and seem to appear unpredictably on the number line. Euclid proved that there were infinitely many primes, but the question is, Where are they? Is there a pattern or rule that can tell where to find them?

In his conjecture, Riemann suggested a formula to describe where the primes are. It involves a certain set of points on a plane that correspond to solutions that make an equation, the zeta function, equal zero. His hypothesis said that all of those points, the zeros of the zeta function, are on a single line. The only exceptions are points that mathematicians call trivial zeros because, they say, everything they care to know about those points is already known.

Riemann, however, gave not a hint of how to prove he was right.

One approach is to prove the conjecture wrong. Over the years, mathematicians have used vast computer calculations to climb further up the line, examining point after point in the infinite collection of points, and so far every point has been on the line. The record is the 10 to the 23d zero, which, as Dr. Andrew Odlyzko of the University of Minnesota discovered, falls on the line, just as 20 billion of its neighbors do.

The physics connection involves the boundary between ordinary Newtonian physics, in which you can know at every moment an object's position and its speed, and quantum physics, the subatomic level where if you know an object's position, you cannot know its velocity, and vice versa.

What happens, physicists asked, in the zone between the worlds of Newtonian

and quantum physics? It turns out to involve the zeta function of the Riemann hypothesis. The distribution of energy levels in highly excited atomic nuclei looks similar to the distribution of the zeros of the zeta function.

This confluence has given mathematicians a promising avenue to explore. But given the history of the conjecture, few express strong optimism.

November 11, 2003

Solution to Old Puzzle: How Short a Shortcut?

By GINA KOLATA

Two mathematicians have solved an old problem in the design of networks that has enormous practical importance but has baffled some of the sharpest minds in the business.

Dr. Frank Hwang of A.T.&T. Bell Laboratories in Murray Hill, N.J., and Dr. Ding Zhu Du, a postdoctoral student at Princeton University, announced at a meeting of theoretical computer scientists last week that they had found a precise limit to the design of paths connecting three or more points.

Designers of things like computer circuits, long-distance telephone lines, or mail routings place great stake in finding the shortest path to connect a set of points, like the cities an airline will travel to or the switching stations for long-distance telephone lines. Dr. Hwang and Dr. Du proved, without using any calculations, that an old trick of adding extra points to a network to make the path shorter can reduce the length of the path by no more than 13.4 percent.

"This problem has been open for 22 years," said Dr. Ronald L. Graham, a research director at A.T.&T. Bell Laboratories who spent years trying in vain to solve it. "The problem is of tremendous interest at Bell Laboratories, for obvious reasons."

In 1968, two other mathematicians guessed the proper answer, but until now no one had proved or disproved their conjecture.

In the tradition of Dr. Paul Erdos, an eccentric Hungarian mathematician who offers prizes for solutions to hard problems that interest him, Dr. Graham offered \$500 for the solution to this one. He said he is about to mail his check.

Add Point, Reduce Path

The problem has its roots in an observation made by mathematicians in 1640. They noticed that if you want to find a path connecting three points that form the vertices of an equilateral triangle, the best thing to do is to add an extra point in the middle of the set. By connecting these four points, you can get a shorter route around the original three than if you had simply drawn lines between those three points in the first place.

Later, mathematicians discovered many more examples of this paradoxical phenomenon. It turned out to be generally true that if you want to find the shortest path connecting a set of points, you can shorten the path by adding an extra point or two.

But it was not always clear where to add the extra points, and even more important, it was not always clear how much you would gain. In 1977, Dr. Graham and his colleagues, Dr. Michael Garey and Dr. David Johnson of Bell Laboratories, proved that there was no feasible way to find where to place the extra points, and since there are so many possibilities, trial and error is out of the question. These researchers and others found ways to guess where an extra point or so might be beneficial, but they were always left with the nagging question of whether this was the best they could do.

The conjecture, made in 1968 by Dr. Henry Pollack, who was formerly a research director at Bell Laboratories, and Dr. Edgar Gilbert, a Bell mathematician, was that the best you could ever do by adding points was to reduce the length of the path by the square root of three divided by two, or about 13.4 percent. This was exactly the amount the path was reduced in the original problem with three vertices of an equilateral triangle.

Knowing Your Limits

In the years since, researchers proved that the conjecture was true if you wanted to connect four points, then they proved it for five.

"Everyone who contributed devised some special trick," Dr. Hwang said. "But still, if you wanted to generalize to the next number of points, you couldn't do it."

Dr. Du and Dr. Hwang's proof relied on converting the problem into one involving mathematics of continuously moving variables. The idea was to suppose that there is an arrangement for which added points make you do worse than the square root of three over two. Then, Dr. Du and Dr. Hwang showed, you can slide the points in your network around and see what happens to your attempt to make the connecting path shorter. They proved that there was no way you could slide points around to do any better than a reduction in the path length of the square root of three over two.

Dr. Graham said the proof should allow network designers to relax as they search for the shortest routes.

October 30, 1990



CHAPTER 4

Chaos, Catastrophe and Randomness

CHAOS THEORY WAS DISCOVERED IN THE 1970s AND 80s, and became something of a household term. But it was used long before that, as a 1938 article makes clear. The article, perhaps a prime example of the dismal state of science writing early in the century, used the word “chaos,” although not in its current sense. “A new mathematical definition of chaos which brings ‘utter confusion’ for the first time under the control of man,” was the way it was described. And the researcher who described a mathematical analysis of chaos? None other than Norbert Wiener, a famous child prodigy who became a professor at the Massachusetts Institute of Technology and founder of the field named cybernetics, which he defined as the science of control and communication. His paper, though, despite the confusing *Times* article, actually was not particularly notable or influential.

But toward the end of the century, in part because of a series of articles in the *Times* by James Gleick, and his best-selling book, *Chaos*, the notion of chaos left the rarefied realm of mathematics and captured the popular imagination. It was sometimes even confused with another buzzword of the time, *catastrophe theory*. Can you predict disasters, experts asked, if they occur only when a sequence of random

events happens to arise? While chaos theory still lives, catastrophe theory fizzled and died, though related questions did not. What is a random event? What are coincidences anyway and how should people interpret them?

Along the way, researchers also started to ask about data mining, the attempt to sift through data and find meaningful patterns. The problem is that there are always patterns, just by chance, in large data sets. So how do you know which are real and which are random noise?

It's an issue that arises over and over again. A cluster of cancers emerges in a town. Does it signal the presence of a potent carcinogen? Or is it a predictable statistical quirk? How would you know?

A sort of mirror image of the search for patterns is the quest for true randomness, streams of numbers that actually have no pattern. Malcolm W. Browne, in an article, explained why that is important: "Mathematical 'models' designed to predict stock prices, atmospheric warming, airplane skin friction, chemical reactions, epidemics, population growth, the outcome of battles, the location of oil deposits and hundreds of other complex matters" rely on a statistical method that requires—absolutely depends on—a string of truly random numbers. The challenge is to find a way of generating those numbers and of showing that they really are random. Not so easy, as Browne explains, and some computer programs that were used to generate strings of random numbers actually were generating strings that had patterns; they were not random.

The answers to all these questions about randomness and chance can be surprising, revealing, and can make you see the world in a different way. At the very least, they may encourage a bit of skepticism. And they may encourage respect for the enormous difficulties that beset scientists venturing into this uncertain territory.

Chaos Is Defined by New Calculus

A new mathematical definition of chaos, which brings "utter confusion" for the first time under the control of man, was reported to the Fourth International Congress for Applied Mechanics here today.

The definition is a new form of calculus. It enables the scientists to predict what will happen in states of complete confusion. Practical uses are many. Examples are the solving of air turbulence which hampers airplane flights and the flow of liquids in pipes.

This calculus was reported by Dr. Norbert Wiener of the Massachusetts Institute of Technology. The mathematics first card indexes sample kinds of chaos. An engineer can select the sample which most nearly resembles his problem.

The steps of a drunken person illustrate the samples. The wobbly walk was one of the problems in chaos which first interested Dr. Wiener. Each step has no relation to previous steps. But calculus can show how far the "drunk" is likely to go in a given time.

Problem in Planets' Motions

"Perturbations" of the planets, their slight, irregular wanderings from their orbits, are a practical example of chaotic movement. Astronomers have been figuring them for centuries, and an explanation by Dr. Albert Einstein of one unexpected motion helped build his fame.

The new definition, Dr. Wiener explained, is entirely mathematical. It defines "pure" chaos. Practical examples of the "pure" state are difficult, he said, but closest to 100 percent chaos are the noises you hear in a vacuum tube, like the radio. Electrons make them, by striking target. But no single electric makes a sound. The racket comes from "mass," that is, when a lot of electrons hit simultaneously.

There are three steps in the new calculus, said Dr. Wiener. The first was the "ergodic" (from the Greek word "ergon," meaning work) theorem of Willard Gibbs, American scientist of the last century. It declared that a chaotic system would run through all possible phases of confusion.

Scientists, said Dr. Wiener, found that the systems did not run the entire gamut.

The next step was by Dr. G. D. Birkhoff of Harvard, with new mathematics by which the time when chaotic events would happen could be averaged.

Adds Factor of Space

Dr. Wiener's word adds "space" to chaos, so as to tell not only the time but the place where a change is likely.

In airplane flights one of the "chaos" troubles is to figure when and where the smooth flow of air over the top of a streamlined wing will break up into eddies, and what kind of eddies. The eddies interfere with the plane's lifting power.

Engineers by experiment measure some of these eddies. But it is impossible to measure them all. Designers have to guess on the basis of their sample eddies. The new mathematics is designed to take the guess work out of these experiments by showing whether the samples are well chosen.

Dr. Norbert Wiener, professor of mathematics at M.I.T. since 1932, received his bachelor's degree from Tufts College in 1909 at the age of 14 and won his Ph.D. at Harvard when he was 18.

September 14, 1938

Experts Debate the Prediction of Disasters

By MALCOLM W. BROWNE

An increasingly bitter debate is spreading among experts in many fields of science over "catastrophe theory"—a mathematical concept intended to explain and predict events as disparate as chemical reactions, dog bites, stock market crashes and the outbreak of war.

General interest in the principle has reached the point that a lecture on the subject at the University of California attracted 1,000 people, and the supply of papers on catastrophe theory is exhausted almost as soon as they are published.

Catastrophe theory is a concept that says the probability that sudden events will occur can be accurately forecast by plotting developments mathematically.

Called Mathematically Unsound

Its proponents say that catastrophe theory promises to predict all kinds of sudden events, even from very small amounts of data, and even if some of the data are wrong.

Critics of catastrophe theory contend that it is mathematically unsound, that it has little or nothing to do with the real world and that predictions drawn from it are so vague and general as to be worthless.

There are eminent mathematicians on both sides of the argument, although the tide seems to have turned in the last year in favor of the critics.

The dispute among mathematics has spread to many fields—biology, social and political science, psychology and other "soft sciences"—where "catastrophists" see potential applications of the principle.

Proponents of the catastrophe theory say that it represents the greatest revolution in mathematical thought since the discovery of calculus three centuries ago.

Catastrophe theory is based on the idea that pictorial representations can symbolize real events.

One of the pictures is the simple line graph, drawn as a two-dimensional figure, which shows how something changes between one state or point and another.

More complex graphs can be drawn on three-dimensional surfaces—spheres, cylinders and paraboloids, for example. Multi-dimensional graphs

contain much more information than two-dimensional graphs, and can represent more subtle changes and relationships.

Topology, the mathematical study of the shapes of surfaces, is the science from which catastrophe theory developed in the mid-1960s, largely because of the work of René Thom, the French mathematician.

Dr. Thom's particular interest was in a kind of surface that folds of surface that folds on itself, changing abruptly from a smooth form to a continuous break of some kind. He postulated that there are seven basic forms of such a curve, and he called the discontinuous break characteristic of all of them a "catastrophe."

Dr. Thom and his followers, especially E. Christopher Zeeman, the English mathematician, proposed that such surfaces, mathematical abstractions in themselves, might serve as suitable models for describing real events, and they set out to prove the idea.

Dr. Zeeman suggested that many real events—a sudden change in a chemical reaction, the sudden buckling of a steel girder, the sudden decision of a dog to attack, the sudden differentiation of growing cells into an embryo—could be represented as "catastrophes" on suitable mathematical surfaces.

Prison Officials Interested

He even asserted that if the right surface were chosen to symbolize the variable factors affecting an event, only a small amount of information would be needed to predict the shape of an entire surface, and from this the event it represented could be predicted.

Among the groups that sought applications in Dr. Zeeman's work was the British prison system. Prison authorities helped Dr. Zeeman in a study he made of the events that had led to a 1972 riot at Gartree Prison, which, he said, could have been plotted on a "catastrophe" surface.

By refining the technique it should be possible, he reasoned, to identify the times and circumstances under which a riot would be likely and to take preventative measures.

Dr. Zeeman published other papers contending that catastrophe surfaces may represent heartbeats, the onset of certain kinds of mental illness and social unrest. For several years, the scientific community appeared to accept these ideas without comment.

But lately, the work of Dr. Zeeman and others has come under increasingly heavy challenge.

A volley of scientific papers by Hector J. Sussman and Raphael S. Zahler, associate professors of mathematics at Rutgers University, was the first concerted attack on the ideas of catastrophe theory. *Science*, a respected American journal, soon followed this with a strong criticism entitled "Catastrophe Theory: The Emperor Has No Clothes."

Dr. Sussman and others accused the catastrophists of trying to intimidate non-mathematicians (and even mathematicians unfamiliar with their work) with such phrases as "deep mathematics."

Catastrophe theory, Dr. Sussman wrote, "is tantamount to claiming that the world can be deduced from pure thought—a claim few scientists would accept."

He added: "Catastrophe theory offers to mathematicians the hope of applying mathematics without having to know anything but mathematics. An appealing dream for mathematicians, but a dream that cannot come true."

Dr. Zeeman has not replied in print to the growing criticism. In an interview with *The New York Times*, he said that his published papers spoke for themselves and that Dr. Sussman's critiques contained "many misquotations, misrepresentations and mathematical mistakes."

Responding to the charge that catastrophe theory is too vague and general to be useful, he asked, "What would you say of numbers, one, two, three, and so forth? They are also general and vague, but would you contend they are not useful?"

"Close Friend for Years"

He said that he was not attempting to prove the utility of catastrophe theory in any field of research, but merely to offer it to others as a tool that they might find useful. In three or four years, he said, social scientists may begin making predictions based on the theory.

But many mathematicians reject even this possibility. Among them is Dr. Stephen Smale, a professor at the University of California and winner of the Fields Medal, the highest recognition that a mathematician can receive. (There is no Nobel Prize in mathematics.)

"I've been a close friend of Chris Zeeman for years," Dr. Smale said in an interview, "and he awarded me an honorary degree at the University of Warwick in Coventry, where he is director of mathematical research.

"But in a sense I reject catastrophe theory completely. It is more of a philosophy than mathematics, and even as a philosophy it doesn't explain the real world. Zeeman's assertions constitute a heavy-handed argument he just cannot justify," Dr. Smale concluded.

Despite such criticism, the number of Dr. Zeeman's supporters appears to be growing in some fields. Dr. Robert T. Holt, professor of political science at the University of Minnesota, is one of them.

"In the social sciences it is terribly difficult to obtain and use exact data of the kind produced by the natural sciences," he said in an interview, "and the catastrophe theory work of Thom and Zeeman offers us a way to get around this.

"For example," he said, "both the beginning and end of the First World War came as big surprises to everyone. Gradual processes suddenly and unexpectedly resulted in the outbreak of the war and the ending of the war. We believe these can be plotted on catastrophe curves of the types proposed by Thom and Zeeman.

"We believe, also, that it would be possible to identify times at which a war would be most probable or least probable using the theory.

"This gives us a mathematical tool which is qualitative as well as quantitative, and I think you have to appreciate the spirit of the theory. Zeeman's papers are clues, not proofs, and we should use them in that spirit."

November 19, 1977

Solving the Mathematical Riddle of Chaos

By JAMES GLEICK

A premature summery Sunday takes Cornell University by surprise, and students head off to sun themselves at Treman State Park. The waterfall trail is closed, supposedly because of hazardous winter conditions. But not everyone is playing by the rules. High above the falls, a man stands at streamside, just where the smooth flow of water begins to speed and shudder. He is sweating slightly in sports coat and corduroys and puffing on a cigarette. Suddenly, in what might be a demented high-speed parody of a tennis spectator, he starts turning his head from side to side, over and over again.

His companions have walked ahead toward the quieter pools upstream, but Mitchell Feigenbaum is totally absorbed. "You can focus on something, a bit of foam or something," he says. "If you move your head fast enough, you can all of a sudden discern the whole structure of the surface, and you can feel it in your stomach." He takes another pull on his cigarette. "But for anyone with a mathematical background, if you look at this stuff, or you see clouds with all their puffs on top of puffs, or you stand at a sea wall in a storm, you know that you really don't know anything."

Here, where the water flashes over the rocks in indistinguishable eddies and cascades, chaos begins, and traditionally that is where science stops. For as long as the world has had physicists inquiring into the laws of nature, it has had a sense of deep ignorance about chaos—disorder, turbulence, in water, in the atmosphere, in the erratic fluctuations of wildlife populations, in the fibrillation of the human heart. The mathematics has simply not existed.

But Feigenbaum, a 39-year-old physicist at Cornell, has become a midwife for a new scientific discipline that is exploring turbulence and disorder of a kind that a decade ago seemed impenetrable. It is built on the discovery that of all the possible paths to disorder, nature favors just a few. It has its own technique of using computers and its own special language. Its practitioners—physicists, mathematicians, chemists, biologists—number no more than a few hundred scientists in the United States and Europe and a few dozen in the Soviet Union and Japan. At the moment, this new discipline doesn't even have a name, just a nickname: chaos.

"Chaos is asking very, very hard questions," says Joseph Ford, Regents Professor of the Georgia Institute of Technology, who organized an influential early conference on the subject in 1977. "It offers the possibility that the answers are going to severely modify our view of the universe. There is a notion that we are beginning to get the microscopic details of how the universe may work."

The growing numbers of researchers in the field hope that chaos will ultimately suggest ways of predicting weather and earthquakes, designing optical computers and jet engines, explaining economic trends and the physiology of the heart. Feigenbaum and his colleagues try to be cautious about predicting real-world applications, and in their cooler moments they emphasize that true turbulence is in some ways as murky as ever. The whole business has a trendy appeal, perhaps trendier than some physicists consider justified. The very notion of order amid chaos, after all, has long been a cliché, applied to all kinds of scientific endeavor.

Academic caution has not discouraged stock-market analysts from showing up expectantly at chaos conferences. Nor, for that matter, has it discouraged program managers in the Departments of Energy and Defense from financing a variety of theoretical projects in the new discipline. Los Alamos National Laboratory has created a Center for Nonlinear Studies to coordinate work on chaos and related problems, and similar institutions are being set up on several university campuses.

"The notion that these phenomena really are very common has led to a whole new birth of investigation of varieties of ways in which systems behave chaotically," says Paul C. Martin, dean of Harvard University's Division of Applied Sciences.

Feigenbaum, a product of Brooklyn and Los Alamos who had trouble getting his early discoveries published, made his first key breakthrough in 1976 and 1977, and in the last few years the word has been spreading in a remarkable round of conferences and symposiums and workshops. This year's Nobel Symposium, beginning tomorrow in Goteborg, Sweden, is devoted to chaos, with an opening address by Feigenbaum. Even so, awareness is just now penetrating the nontechnical segments of the academic world. "The folk in the academic community are beginning to recognize that there's something called chaos," Ford says. "They're not sure if they like it or if they'd prefer it would go away, but they know something's afoot."

Chaos seems to be everywhere. It's in a rising column of cigarette smoke that suddenly breaks into wild swirls. It's in a dripping faucet that goes from a steady

pattern to a random one. "It's in the behavior of the weather, the behavior of an airplane in flight, the behavior of oil flowing in underground pipes," says Kenneth G. Wilson, professor of physics at Cornell. They behave in strikingly similar ways. The actual stuff that is disorderly seems to matter less than the disorder itself.

Wilson's Nobel Prize-winning work in physics in the 1960s provided a springboard for Feigenbaum, who made his own discoveries at Los Alamos National Laboratory. Using a calculator and then a series of desktop computers, Feigenbaum found regularities in the behavior of some simple mathematical equations when they were worked over and over again, with the results being fed back into the equations as input. The equations could be manipulated to produce, first, orderly strings of numbers—series with recognizable logic—and then disorderly ones. As Feigenbaum watched the numbers turn from orderly to disorderly, he began to see patterns in the transition, and the patterns were pretty, the way such things are pretty to a mathematician with an eye for unexpected simplicity.

At first, Feigenbaum and his colleagues assumed that the patterns had something to do with the particular equations he was examining. But to their enduring surprise, completely different equations seemed to produce the same patterns in the transition to disorder. A mathematical description of these patterns always seemed to involve certain particular numbers, now known informally as Feigenbaum numbers. The patterns seemed to have universality, and universality was magic.

Even then, Feigenbaum's work might have made no more than good dinner-table conversation, without lasting significance. Indeed, the scientific journals wouldn't touch the articles he offered them. But the state of things in a half-dozen different fields made the time right for his discovery. The implication was that if these regularities were universal, they would appear in real systems governed by mathematical equations far more complicated than the ones Feigenbaum had explored—equations for the motion of fluids or the change in animal populations. And sure enough, Feigenbaum's computer patterns turned up in 1978 experiments with fluids in France. The news traveled fast.

"You get these subjects that become popular when one person makes a breakthrough that makes it possible to do a lot of research in an area," Wilson said. "Here the breakthrough was Feigenbaum's work, finding a way to study the borderline between organized behavior and chaotic behavior."

A few of Feigenbaum's colleagues now believe they are seeing the beginnings of a true course change for physics. The field has been dominated for two

generations by the glittering abstractions of high-energy particles and quantum mechanics. The achievements have changed the 20th-century landscape, beginning with the atom bomb and nuclear power. But to some—especially younger physicists—progress year to year is beginning to seem slow, the naming of new particles is beginning to seem empty, the body of theory is beginning to seem cluttered. There has long been a feeling, not always expressed openly, that theoretical physics has strayed far from human intuition about the world.

Whether this will prove to be fruitful heresy or just plain heresy, no one knows. But some of those who think physics may be working its way into a corner are looking to chaos as a way out. They like the feel of it. For one thing, it has a crisp mathematical quality that recalls Newton's revolution in physics. For another, it opens a window on the great gulf between knowledge of what one thing does—one water molecule, one bit of heart tissue, one neuron—and what millions of them can do.

Watch two bits of foam flowing side by side at the bottom of a waterfall. What can you guess about how close they were at the top? Nothing. As far as mathematics is concerned, God might just as well have taken all those water molecules under the table and shuffled them personally.

Physicists always assumed that when they saw such a random relationship between what goes into a system and what comes out, the randomness had to be part of the system, in the form of noise or error. In a way, the modern study of chaos began with a creeping realization in the 1960s that quite simple mathematical equations produced results every bit as violent as a waterfall. Tiny differences in input could quickly become overwhelming differences in output—a phenomenon given the name "sensitive dependence on initial conditions." In weather, for example, this translates into what is only half-jokingly known as the Butterfly Effect—the notion that a butterfly flapping its wings today in Peking might affect the weather next month in New York. It is not a notion designed to give comfort to long-range forecasters.

Understanding of the Butterfly Effect began with Edward N. Lorenz of the Massachusetts Institute of Technology, who worked out many of the unimagined properties of these systems. But his work was published mainly in meteorology journals, and few physicists appreciated the consequences of it even five years ago. For scientists who had not actually played with the equations themselves, the notion could be deeply implausible.

"You'd get up and give a talk about sensitive dependence on initial conditions in front of a physics department," recalls J. Doyne Farmer, now a Los Alamos physicist, "and people would say, 'Well, are you sure this isn't just numerical error?' You'd get a lot of, even, hostility." Farmer was one of a group of graduate students in physics at the University of California at Santa Cruz who got so caught up in the excitement of chaos that they dropped their earlier specialties cold, to the dismay of the faculty. They thus entered a small but growing body of chaos lore as the "Santa Cruz Dynamical Systems Collective."

For biologists, among others, all this was interesting. Consider for example, a population of fish. In a limitless ocean, it might grow smoothly from year to year, and biologists could describe the change with a mathematical model using a linear equation. But to make the model one step more realistic, biologists might look at fish in a pond. There, if one begins with just a few fish, the population grows; when there are too many for the amount of food, it declines. That one twist makes the system nonlinear. The waxing and waning of the fish population can still be described quite simply by an equation, repeated over and over again to calculate the change from generation to generation, but the equation can do startling things.

It could be that, no matter how many fish you start with in the pond, the population eventually settles down to a stable number, like a pendulum making shorter and shorter swings until it comes to a halt. But a few biologists, attuned to the mathematical developments of the 1960s and 70s, saw the other possibilities. One of them was Robert M. May, professor of biology at Princeton University.

"Most of our intuitions formed in mathematics or physics courses are that, if you have a fairly simple description of something, then it's going to describe fairly simple behavior," May says. "But if you take a population that is more boom-and-bust in its dynamics, you find that it doesn't do something simple as you thought."

Working out the results on a computer, a scientist could alter the model, slowly changing one variable in an equation to make it represent a more boom-and-bust fish population, like turning a knob to raise the heat under a pot of boiling water. After a certain point, the population might start to oscillate, settling down not to one stable number but to two different numbers in alternating years. Then, as the boom-and-bust variable changed further, the period of oscillation might change to four years, then eight, and so on until suddenly the population became completely erratic, changing year by year in

an unpredictable way. That pattern, called "period doubling," is now recognized as one fundamental kind of transition to chaos.

The real world, of course, does have randomness and noise that don't figure in an idealized calculation of this kind—a fish population might depend on a hundred different variables, beginning with the weather. But period doubling did turn up in experiments with fluids. A half-inch cube of liquid, for example, is slowly heated from below. The warm liquid rises in a smooth rolling motion. Then, as the temperature difference is increased, wobbles appear in the rolls, and then wobbles in the wobbles. A probe, measuring the speed of the liquid at a given point, finds first a constant speed, then an oscillation between two speeds, each repeating itself, say, once a second. Then the two speeds split to four, each showing up half as often, and so on, until chaos sets in.

"The world of biology out there outside the laboratory really has so much environmental noise and so much interaction among species that I don't look to see the crisp patterns, the Feigenbaum numbers, appearing the way they do in physics," May says. "And yet I think that many of the oscillations you see in the real world are oscillations of the kind that are latent in these nonlinear sorts of equations." Some of his colleagues are even more optimistic, expecting chaos to help in understanding cycles in measles epidemics or predator-prey populations.

May published an intriguing article about all this in *Nature* in 1976, exhorting his colleagues to look at the odd behaviors that develop when simple equations act upon themselves over and over again, and to teach their students about them. "It was biologists who said, 'Hey, this is really important—deterministic models do mad things,'" he says. "Mitch went one step further and said, 'Not only do they do mad things but there are important regularities you might look for and take seriously.'

"It's not enough to have an idea, you've got to understand how important it can be. And even if you've noticed how important it is, if there isn't an audience of people ready to listen to you, it doesn't matter." In 1976, the audience was not quite ready.

Sometime in 1974, the physicists in the Theoretical Division at Los Alamos became aware that their new colleague was working 26-hour days, which meant that his waking schedule was slowly rolling in and out of phase with theirs. It also meant that he was taking long, lonely walks in the starlight that hammers down through the thin air of the mesas, and this sometimes distressed the local police. He was an unusual case. He had exactly one published article to his name, he was

working on nothing that seemed to have any particular promise, yet, at the age of 29, he had already become a sort of resident savant among the savants.

"He acquired the reputation of being the superbright person you went to see when you couldn't figure things out," says Peter A. Carruthers, a senior fellow of Los Alamos who was then head of the division. "He became the perfect consultant, and when people could find him, they would bring him problems about anything at all."

Some of his friends, though, were wondering whether he was ever going to produce any work of his own. As willing as he was to do impromptu magic with their problems, he didn't seem interested in devoting his own research to any question less cosmic than, say, What is time?

Mitchell Jay Feigenbaum was born Dec. 19, 1944, in Philadelphia, where his father was a chemist in the Navy Yard, eradicating cockroaches on ships bound for the Pacific. After the war, his parents moved back to the Flatbush section of Brooklyn, his father working for the Port of New York Authority and then for Clairol and his mother working as a teacher in the public schools. Soon enough, the mystery of the universe announced itself to Feigenbaum through a Silvertone radio sitting in the living room.

"Every morning at 5:30 or 6 it would play," he says. "For some reason it struck me as strange that it could make music with nothing coming in. Was remarkable. Because I understood phonograph at that point, when I was 4 or 5 my grandmother gave me a special dispensation that I could put on the 78 records." When Feigenbaum talks, his passionate eyes opening like electronic shutters in sudden darkness, his hair sweeping stochastically back from his brow in the style of busts of German composers, he tends to start dropping certain articles and pronouns. "But the radio made music with nothing coming in, and it struck me to understand that was deepest thing in the world. It's not the stuff of wisdom, but maybe one can be struck by anything. In fact, even now, I don't know the answer."

Growing up smart, through Samuel J. Tilden High School and City College, was in some measure a matter of steering an uneven course between the world of mind and the world of other people. "First I was immensely social when I was little. People would come wanting to beat me up; it's a matter of course living in Brooklyn, and I would convince them that they should become my friend. I never fought when I was little, never, I completely avoided. And then suddenly in second grade, something clicked, and I realized I could learn things. But somewhere I started losing all my friends.

"By college I had none, working at night and totally preoccupied, and I completely missed puberty and adolescence and everything. But my last term, I realized I had some improvement to do, so I started showing up in the cafeteria. I would listen to people talking about incredible nonsense. There was this fellow talking about how his shaver could never give him a close shave, but when he took the head off it it worked much better. I just sat myself down and forced myself to listen to that, and after a few months, I began to be able to talk to people. It was a serious thing. I realized I had completely lost contact with the world."

His choice of specialties began pragmatically. "When I was 10 or 11, it was known in the air in Brooklyn, first of all that electrical engineers worked on radios, and second that an electrical engineer could maybe get a job and earn a salary. In college, it grew clear that what I wanted to know about a radio was more apt to be in physics.

"I always had a feeling that all things of humanities were pleasant things, but somehow they were what you're supposed to know just by being a person. But the mathematical and scientific stuff, that was work, and that was how you contributed to the human race. I don't know how I thought such a mishegoss."

Feigenbaum graduated in 1964 and went on to M.I.T., where he got his doctorate in elementary particle physics in 1970. Then he spent a fruitless four years at Cornell and at the Virginia Polytechnic Institute—fruitless, that is, in terms of the steady publication of work on manageable problems that is essential for a young university scientist. In his own mind, he still believes this was a time when he did the best thinking of his life, on the most profound questions, but it led nowhere. He had nothing to show—it was all, as he says, loose and floppy. He believes that his career was almost lost. But Peter Carruthers, who knew him at Cornell as perhaps the most talented young student he had ever seen, brought him to Los Alamos.

When inspiration came to Feigenbaum, it was in the form of a picture, a mental image of two small wavy forms and one big one. That was all. He had been working for months on the problem of period doubling, running numbers through a Hewlett-Packard calculator for hours on end, then moving on to a big Control Data computer, and he had discovered his first universal constant. It is an expression of how exactly rapidly a system undergoes period doubling on its way toward chaos—always. It is 4.669201609

When Feigenbaum discovered this number, he did what any mathematician would do. He calculated it to great precision and tried multiplying and dividing

different combinations of other well-known constants, π and e and others, to see if his number was related somehow. It didn't seem to be, and for months he couldn't shake a suspicion that somehow he was still missing the point. He felt as though fate had dropped a jewel in his lap and he didn't know what to do with it.

Then, at lunch one day, that vague wavy image came to him—no more, perhaps, than the visible top of a vast iceberg of mental processing that had taken place below the waterline of consciousness. It had to do with scaling, the way the small features of a thing relate to the large features, and it gave him the path he needed. Scaling, as Kenneth Wilson had discovered a decade before, can let you throw out a lot of unnecessary information and focus on what truly describes the essence of a structure. For period doubling, scaling showed not only when one value—a total population or a fluid speed—would break into two, but also just where the new values would be found. Scaling was an intimate feature of the peculiar world Feigenbaum was beginning to explore.

It is a world that depends on the existence of computers as no discipline ever has before. For Feigenbaum, to begin with, the computer was a way to bridge a professional gap between theory and experimentation. For particle physicists, any experiment is costly in time, money and technical sophistication. But to explore the realm of partial differential equations, Feigenbaum and others have made the computer their own accelerator, cloud chamber and camera all in one.

Early users of computers discovered that problems which could not be solved directly could often be simulated, and simulation has become a standard technique for things like weather forecasting. Given the weather at one time at thousands of points, and given equations for how weather changes, a computer can simulate the changes and see what happens. That is useful for certain problems; it is a powerful technique. Unfortunately, it is a complicated world. No existing computer, and no computer that will be built soon, can calculate enough points with enough speed to handle a rich system for long, which is why you are almost as well off flipping a coin as reading the forecast in today's paper for Thursday's weather.

Even if computers could be made unimaginably powerful, someone would still have to gather information more nimbly than is possible with satellites and balloons. And even if that could be managed, there is still the Butterfly Effect.

Feigenbaum's technique, although it owes something to the spirit of simulation, is quite different. He does not use computers so much to solve problems as to explore them. He wants to develop intuition, the way an outfielder has

developed intuition about fly balls by watching thousands of them sail skyward.

"It's a way to go in and probe a problem," Feigenbaum says. "You look at something, you see what comes out and you figure out a little better what was going on. It isn't a way to get a careful set of data—the data, in fact, aren't even interesting. The idea is to hone in and see what are the principles. Each one of these problems that you start playing with, each one is slightly more complicated than the next. There are surprises in each of them, and one has to learn the repertoire of what these things do."

It can be a dauntingly esoteric, yet surprisingly basic. If you tune in for a moment to Feigenbaum describing his work to what he thinks of as a general audience, you might hear something like this: ". . . and all it is is a Duffing's equation—this is a damped, driven, anharmonic oscillator. It's a quartic postential, so just an x -cubed force law, I haven't even put in a linear term there, it's explicitly dissipative. . . ."

But he might just as well be talking about a child getting pushed on a playground swing. It is easy for a mathematician to describe what happens, with just a few traditional equations. The swing gets a regular push, it accelerates down, decelerates up, loses a bit to friction, gets another push. The motion can quickly settle down to a pattern, with the swing coming to the same height each time. But, odd as it seems, the motion can also turn out to be utterly unpredictable.

The unpredictability comes from two essential features of this simple system—each producing a little mathematical twist, and each shared by the more interesting systems of nature, like the weather. The swing is damped, and it is driven: damped because friction is trying to bring it to a halt, driven because it is getting a periodic push. The weather is damped and driven in the same way, always losing energy through friction and dissipation of heat to outer space, and always getting a push from the sun.

Traditional mathematics can't answer the easiest questions about the future of a child's swing—how fast the swing will travel on average, how many times an hour the swing will get at least four feet off the ground. A computer can look at the problem by simulating it, rapidly calculating each cycle. But the tiny imprecision built into each calculation builds up, because this is a system with, yes, sensitive dependence on initial conditions. Before long, a simulation of even this trivial example starts to require immense computer power.

Feigenbaum uses his computers to poke around in systems like this, changing the friction or the force or the timing to see what happens. A screen that turns

the data into color pictures is his way of allowing quick, intuitive recognition of patterns. At Los Alamos, despite the presence of the world's finest supercomputers, it took him months to get the kind of graphics equipment he needed. The only appropriate terminals were in high-security areas—"behind the fence," in the local parlance—and finally the Theoretical Division had to buy him one, disguising it budgetarily as a \$20,000 "desktop calculator."

Now, having left after an unhappy divorce ended a two-and-a-half-year marriage and made Los Alamos too small for comfort, he has one small computer in his apartment in Ithaca, N.Y., and a \$100,000 model, paid for by the Army, in his Cornell office. He has customized them to run a version of Basic—a well-known language that encourages an interactive, trial-and-error style—jazzed up with some fast machine-language routines of his own. He is using them to explore systems with more complicated possibilities than the relatively simple ones he started with.

Watching Feigenbaum work can be mesmerizing. It is, first of all, a process of continual abstraction, winnowing out unnecessary detail to isolate the essentials. There is no need to chart the whole history of a system like a child's swing, for example—one need only look at the top of each cycle. So Feigenbaum might begin by placing a point on a blank screen, its east-west position representing one variable, its north-south another. The computer picks up the dot and runs with it, tracing, perhaps, a closed curve that loops back on itself. Start somewhere else and the computer traces a different curve—the curves representing a regularity in the system that might have been hard to perceive directly. Somewhere else, and the dot remains stationary, representing a perfectly regular cycle that doesn't change from swing to swing. When Feigenbaum is done, he has a multicolor map of the system's behavior, with areas of recognizable pattern and areas of disorder, dots sprinkled randomly. For some systems, a very special sort of map can appear. It is known as a strange attractor, and it has become a kind of emblem for the whole discipline. A strange attractor isn't drawn smoothly. It begins with dots jumping about erratically, until a pattern starts to take shape gradually, as if appearing out of the mist. It is a kind of curve folded in upon itself over and over again.

The strange attractor has two odd qualities. Because it is made up of points scattered in an unpredictable order, two points close together on the curve may have begun unpredictably far apart—another example of sensitivity to initial conditions. But it is the second quality, a scaling quality, that has captured many scientists' imaginations. When a piece of a strange attractor is magnified, it

shows detail that was at first invisible. When the detail is magnified, even more detail appears, in patterns of infinite depth. The closer one looks, the more the curve seems to be repeating itself at smaller scales, like an unending sequence of Russian dolls one inside another. Or like the puffs upon puffs upon puffs in a cumulus cloud, or the whorls within whorls in a turbulent stream.

"What Mitchell has done," said Doyne Farmer of Los Alamos, "is build a mathematical analogue of a microscope. It allows you to look at iterated functions, to zoom in on certain pieces of them and blow them up, and to do that over and over again. You can use this microscope to see what the fine structure of these equations looks like."

Feigenbaum's first papers from Los Alamos, in 1976 and 1977, were returned unpublished. It didn't matter. "In truth, the dissemination of information no longer goes through journals," Feigenbaum says. "It all goes through a well-supported preprint system." Indeed, in the age of photocopying, scientists have mailing lists for their papers, and staying current is very much a matter of making sure you are on the right mailing lists. Even now, Feigenbaum's complete published works would barely fill a small book. Still, he has managed to save every rejection letter.

A 1977 conference in Como, Italy, organized by Joseph Ford of Georgia, was a turning point. "It became clear that somewhere a time had become right for such a subject," Feigenbaum says. "People weren't necessarily there to understand about fluids, or about particle physics, but about all sorts of curiosities that were arising in nonlinear problems."

Ford himself remembers it as a kind of epiphany. "In disciplines from astronomy to zoology, people were just publishing in their narrow disciplinary journals, totally unaware that the other people were around. In their own areas, they were regarded as a bit eccentric. But if you just changed the words, they were all doing the same thing. These people were just weepingly grateful to find out everybody else was there. Mitch's talk was the highlight of the meeting. It was one of those things whose time had come."

Dr. Richard J. Cohen at M.I.T. is working on what he believes is probably the main health problem for Western society. Robert Shaw at the Institute for Advanced Study is on the verge of finishing a long-awaited paper on the physics of a dripping faucet.

Cohen, who holds a joint appointment in the Harvard-M.I.T. Division of Health Sciences and Technology and in the M.I.T. physics department, has developed a novel approach to the chaos that develops in the human heart in

hundreds of thousands of cardiac deaths each year in this country. About half the time, chaos in the heart—ventricular fibrillation—comes after a blocked artery causes the death of tissue. But half the time, the cause appears to be only some kind of electrical instability.

With animal experiments, and with a computer model, Cohen and several colleagues are exploring the circumstances in which the heartbeat begins to disintegrate until the heart is no longer pumping blood. Their hope is to develop ways of identifying people who are at risk before, as Cohen says, “the catastrophic event occurs.” They have already observed period doubling and some of the other classic patterns in the onset of chaos.

“We’re trying to approach this problem from a very different perspective than has been done traditionally,” he says. “It is a clear instance of the Feigenbaum phenomenon, a regular phenomenon which, under certain circumstances, becomes chaotic, and it turns out that the electrical activity in the heart has many parallels with other systems that develop chaotic behavior.”

The dripping faucet, for example. Shaw, a physicist who is another product of the Santa Cruz Collective, has been studying it for several years as a theoretical paradigm of chaos. He, too, has both a computer model and an experimental setup—in his case a brass nozzle with a plastic tub of water above it. The drops of water interrupt a beam of light, to measure the intervals precisely, and the whole thing is controlled by a little computer.

A slow drip can be quite regular, each drop a little bag of surface tension that breaks off when it reaches a certain size. But the size of the drop changes slightly depending on the speed of the flow and depending on whether there is a little rebound from the drop before. And that is enough to make the system nonlinear.

“If you turn it up you can see a regime where the drops are still separate but the pitter-patter becomes irregular,” Shaw says. “As it turns out, it’s not a predictable pattern beyond a short period of time.”

It also shows sensitivity to initial conditions, so vibration has been a serious issue. Shaw found himself doing much of the work at night, when people would be less likely to be tramping by in the corridor. “Unfortunately,” he says, “it turns out that the thing is an excellent seismometer.”

For some scientists, there is reason to pause when they explore systems as simple as a faucet and find that they are, as Shaw says, eternally creative.

Practically speaking, it means that scientists have to think differently about the problems of nature. It changes their intuitions about what the answers can

look like, and that changes the questions they ask. Chaos becomes a technique for doing science—but it also becomes a conceptual framework on which theoreticians can hang some of their most treasured suspicions about the workings of the universe.

To some physicists, chaos seems like a kind of answer to the problem of free will. The realization that the simplest, most deterministic equations can look just like random noise suggests—philosophically, at least—that the Calvinists' deterministic view of the world can be reconciled with the appearance of free will. To people like Ford, chaos is also something like a death knell for the probabilistic ideas of quantum mechanics. "Chaos makes it absolutely clear what the limits are," he says. Last year he gave a talk titled, after Einstein, "Does God Play Dice with the Universe?"

"The answer is yes, of course," he says. "But they're loaded dice. And the main objective of physics now is to find out by what rules were they loaded and how can we use them to our own ends."

To some artificial intelligence specialists at the Institute for Advanced Study and at Los Alamos, chaos suggests a means of linking the simple behavior of neurons to the unpredictable behavior of brains. And to Feigenbaum himself, it is at least a glimpse of a way to link the analytic achievements of his profession to his intuitions about the world.

In the last few years, he has begun going to museums to look at how artists handle complicated subjects, especially subjects with interesting texture, like Turner's water, painted with small swirls atop large swirls, and then even smaller swirls atop those. "It's abundantly obvious that one doesn't know the world around us in detail," he says. "What artists have accomplished is realizing that there's only a small amount of stuff that's important, and then seeing what it was. So they can do some of my research for me. "I truly do want to know how to describe clouds. But to say there's a piece over here with that much density, and next to it a piece with this much density—to accumulate that much detailed information, I think is wrong. It's certainly not how a human being perceives those things, and it's not how an artist perceives them. Somewhere the business of writing down partial differential equations is not to have done the work on the problem."

He is sitting at a small table in his bare Ithaca apartment. There is also a bed, his computer, a formidable record collection, two massive speakers and virtually no other furniture. He stubs out one cigarette and lights another. "One has to look for different ways," he says. "One has to look for scaling structures—how do big

details relate to little details. You look at fluid disturbances, complicated structures in which the complexity has come about by a persistent process. At some level they don't care very much what the size of the process is—it could be the size of a pea or the size of a basketball. The process doesn't care where it is, and moreover it doesn't care how long it's been going. The only things that can ever be universal, in a sense, are scaling things.

"In a way, art is a theory about the way the world looks to human beings. Somehow the wondrous promise of the earth is that there are things beautiful in it, things wondrous and alluring, and by virtue of your trade you want to understand them." He puts the cigarette down. The smoke rises from the ashtray, first in a thin column and then, in a small gesture to universality, in broken eddies and tendrils that continue swirling upward to the ceiling.

June 10, 1984

The Man Who Reshaped Geometry

By JAMES GLEICK

Newton never said it, nor Galileo, nor Freud. The historian of science I. Bernard Cohen scoured the annals of discovery for scientists who announced that their own work was revolutionary, but he could produce only this short list: Symmer, Marat, Lavoisier, von Liebig, Hamilton, Darwin, Virchow, Cantor, Einstein, Minkowski, von Laue, Wegener, Compton, Just, Watson and Benoit Mandelbrot. Sixteen visionaries and cranks—and on a bright windless day it is the latest and last-named who appears in Woods Hole, Mass., ready to propagate his particular revolution at a scientific lecture and clambake.

He tours the Woods Hole Oceanographic Institution, mildly annoyed that his lecture has been left off the printed calendar of events. He steps into the auditorium, briefly intercepted by a young woman pressing her father's business card into his hand. The calendar notwithstanding, every seat is taken. In the front row, three researchers puzzle over *Scientific American's* computer pictures of the "Mandelbrot set," a numerical construct billed as the most complex object in mathematics. He listens to his introduction ("... taught economics at Harvard, engineering at Yale, physiology at the Einstein College of Medicine. . ."). He clips a microphone onto the front of his short-sleeved shirt and begins confidently: "Very often when I listen to the list of my previous jobs, I wonder if I exist. The intersection of such sets is surely empty." Indeed, for three decades, Benoit Mandelbrot failed to exist in a long list of different fields. He was always an outsider, taking an unorthodox approach to an unfashionable corner of mathematics, exploring disciplines in which he was rarely welcomed, hiding his grandest ideas to get his papers published—surviving mainly on the confidence of his colleagues at I.B.M.'s Thomas J. Watson Research Center in Yorktown Heights, N.Y.

But now, at the age of 61, he can watch his revolution advance. Mandelbrot has invented a new way of describing, calculating and thinking about shapes that are irregular and fragmented, jagged and broken up—shapes like the crystalline curves of snowflakes or the discontinuous dusts of galaxies. He had an insight into an organizing structure that lies hidden among the hideous complication of such shapes—an insight that is now transforming the way scientists look at the natural world, and what they find when they look.

Within a decade, Mandelbrot's discovery has evolved from an oddity into a full-fledged science, providing a new language for talking about a particularly rich part of the universe. His tools have been taken up by physicists, chemists, seismologists, metallurgists, probability theorists, physiologists and economists. They are discovering applications in areas ranging from the search for underground oil deposits to the creation of polymers and the strengthening of steel. A new geometry has emerged, and it turns out to be nature's own.

The shapes of classical geometry are lines and planes, circles and spheres, triangles and cones. They represent a powerful abstraction of reality, and they inspired a powerful philosophy of Platonic harmony. But for some kinds of complexity, they turn out to be the wrong kind of abstraction.

Clouds are not spheres, Mandelbrot is fond of saying. Mountains are not cones. Lightning does not travel in a straight line. The new geometry mirrors a universe that is rough, not rounded, scabrous, not smooth. It is a geometry of the pitted, pocked and broken up, the twisted, tangled and intertwined.

The understanding of nature's complexity awaited a suspicion that the complexity was not just random, not just accident. It required a faith that the interesting feature of a lightning bolt's path, for example, was not the straight line denoting its direction, but rather the distribution of its zigs and zags. Mandelbrot, beginning three decades ago, has dusted off some obscure mathematics that now illuminate these special kinds of complexity. He makes a claim about the world, and the claim is that such odd shapes carry meaning. The pits and tangles may be more than blemishes distorting the classic shapes of Euclidean geometry. They may be the keys to the essence of a thing.

To name the structures he was isolating, Mandelbrot rummaged through his son's Latin dictionary one winter's afternoon in 1975 and coined the word "fractal," to connote both fractured and fractional.

Suddenly, fractals are everywhere. In physics and other fields, fractals conferences have become the rage. Scientists in some fields find the concept simply a convenience. Others, with a more hard-core attitude, have formed a cadre that one physicist calls a "fractals mafia." The Department of Defense and private industry are putting more and more money into fractals research.

Mandelbrot himself, an I.B.M. Fellow and now also professor of the practice of mathematics at Harvard, has lately gathered many honors, including, this year, the Barnard Medal for Meritorious Service to Science. It is awarded every five years by the National Academy of Sciences under the administration of Columbia

University for the most worthy "discovery in physical or astronomical science" or "novel application of science to purposes beneficial to the human race."

Yet he remains a peculiar sort of genius. He is reviled by some colleagues, who think he is unnaturally obsessed with his place in history. They complain that he hectors them bitterly about giving due credit. Unquestionably, in his years as a perpetual heretic he honed an appreciation for the tactics, as well as the substance, of scientific achievement. As a Polish émigré in France, and then as a French émigré in the United States, he missed chunks of basic schooling, and he has remained on the periphery of the traditional dogmas—at home nowhere. In field after field, his insights were of a kind that might have been possible only for an outsider.

"From the very beginning, his angle has been to show people that they were making faulty assumptions simply because they didn't have the tools to look beyond them," says David B. Mumford, professor of mathematics at Harvard. "They had missed a whole range of things. Mandelbrot's idea was that you could draw a thing, and that by drawing it you suddenly became aware of what was really going on. And the things he drew, I don't think that even he anticipated that they would turn out to be so strikingly beautiful."

Above all, he is a geometer. Where the main channels of mathematics have favored analysis—the manipulation of functions and the solving of equations—Mandelbrot's way of thinking has always been visual, spatial, turning abstract problems into vivid, recognizable shapes. His work almost depends on its esthetic quality. "Geometry is sensual, one touches things," Mandelbrot says. "I see things before I formulate them."

In a compartmentalized academic world, a common tide can remain unfelt, and the recognition of a new kind of complexity has been developing slowly in many disciplines for nearly a generation. Mandelbrot's work on fractals is a part of the revolution in understanding chaos, the study of turbulence and disorder in a whole range of phenomena. The unifying ideas have brought together scientists who thought their own observations were idiosyncratic, and who had no systematic way of understanding them.

Now they see universality. The insights of fractal geometry help scientists who study the way things meld together, the way they branch apart, or the way they shatter. It is a way of looking at materials—the microscopically jagged surfaces of metals, the tiny holes and channels of porous oil-bearing rock, the fragmented landscapes of an earthquake zone. A new kind of symmetry has emerged, not of

left-to-right or front-to-back but of small-scale patterns to patterns on larger and larger scales—the self-similarity of a broccoli floret whose tiny bifurcations echo the branching of the stalk as a whole.

Fractals also describe the way things cluster in space and time—the distribution of galaxies, of Saturn's rings, of (as one Japanese physics paper contends) cars on a crowded highway. Mandelbrot made his most important early leap of imagination when, at I.B.M., he was asked to examine the problem of “noise,” unexplained errors, in electronic transmission lines. It was a nasty and expensive problem for the resident experts. The errors were not completely random—they tended to come in bunches, and Mandelbrot realized that the degree of bunching remained constant whether he plotted them by the second or by the hour. Oddly, the patterns that arose, and the mathematical description of them, seemed to apply just as well to very different problems, from fluctuating cotton prices back through the 19th century to the rising and falling of the River Nile through two millennia.

Things wear their irregularity in an unexpectedly orderly fashion. They have self-similarity on different scales. When you zoom in, looking closer and closer, the irregularities don't smooth out. Rather, they tend to look exactly as irregular as before.

Mandelbrot himself believes that the notion of self-similarity strikes ancient chords in our culture. Indeed, an old strain in Western thought honors the idea, going back to Aristotle. Leibniz imagined that a drop of water contained a whole teeming universe, containing, in turn, water drops with new universes within. “To see a world in a grain of sand,” Blake wrote, and often that was just what scientists were disposed to see. When sperm were first discovered, each was thought to be a homunculus, a tiny but fully formed human.

But self-similarity withered as a scientific principle, and for a good reason. It just didn't fit the facts. “The complete failure of this great old myth of self-similarity led to the opposite view,” Mandelbrot says, “that as you look closer, each time the world changes. I don't pretend that atoms are like small solar systems—they're not. But what I bring back in is a return to the old myth where it is applicable.”

The peculiar kinds of structures that display self-similarity often seem to have been repeatedly folded in upon themselves, so that the more one magnifies them the more detail they show. Mandelbrot likes to quote Jonathan Swift: “So, naturalists observe, a flea/ Hath smaller fleas that on him prey;/ And these have smaller still to bite 'em;/ And so proceed ad infinitum.”

Self-similarity can lead to some seeming paradoxes. Mandelbrot put one forward when he asked, in the title of an early technical article, "How Long Is the Coast of Britain?"

"People usually give two answers," he says. "Either 'I don't know, it's not my field,' or 'I don't know, but I'll look it up in the encyclopedia.'"

In fact, it depends on the length of your ruler. As the scale becomes finer and finer, bays and peninsulas reveal new subbays and subpeninsulas, and the length—truly—increases without limit, at least down to atomic scales.

"You're used to mathematics that characterize objects that are fundamentally smooth," says Ralph E. Gomory, head of research for I.B.M., who encouraged Mandelbrot's work on fractals when it was least fashionable. "Yet these things model a tremendous class of physical phenomena. It really enables us to realize the unity that is out there."

It is hard to break the habit of thinking of things in terms of how big they usually are, how long they usually last. A hurricane, for example, is a storm of a certain size by definition. But the definition is imposed on nature. In reality, atmospheric scientists are realizing that tumult in the air forms a continuum, from the gusty swirling of litter on a city street corner to the vast cyclonic systems visible from outer space. The message of the new geometry is that such categories mislead—that the ends of a continuum are of a piece with the middle, where one finds storms like the violent rain cell last August, small and short-lived enough to elude the detectors at Dallas-Fort Worth Airport, but intense enough to bring down Delta Flight 191.

Blood vessels, from aorta to capillaries, form a continuum. They branch and divide and branch again until they become so narrow that blood cells are forced to slide through single file. They fill the three-dimensional space of the human body so efficiently that in most tissue no cell is ever more than three or four cells away from a blood vessel. It's the Merchant of Venice syndrome, as Mandelbrot points out—not only can't you take a pound of flesh without spilling blood, you can't take a milligram. Yet the vessels and blood themselves take up little space, no more than about 5 percent of the body's volume. As a design feature, that is important, because blood is physiologically costly. The value of fractal geometry to physiologists is that it provides a way of measuring the branching, a way of calculating a number that predicts how rapidly vessels will divide on smaller and smaller scales.

The key is that, mathematically speaking, fractals are shapes with fractional dimensions—a notion that turns out to have useful practical results, even though

it is impossible to visualize. For shapes with the infinite convolutions of fractals, the number of dimensions expresses the ability to fill space, in a sense. A curve with 1.3 dimensions, for example, lies somewhere between a one-dimensional line and a two-dimensional plane. The greater the dimension, in effect, the greater the degree of complexity and roughness.

"I started looking in the trash cans of science for such phenomena, because I suspected that what I was observing was not an exception but perhaps very widespread," Mandelbrot says.

"I attended lectures and looked in unfashionable periodicals, most of them of little or no yield, but once in a while finding some interesting things. In a way it was a naturalist's approach, not a theoretician's approach. But my gamble paid off."

Around the turn of the century, some mathematicians realized that it was possible to construct shapes with peculiar properties like infinite self-embeddedness.

Imagine a simple triangle, each side one foot long. Now imagine a transformation in which a new triangle, identical but smaller, is fitted onto the middle third of each side. The result is a Star of David. The shape's border now has 12 segments totaling four feet in length—the transformation has lengthened the border by one-third.

If the transformation is repeated on each of the 12 sides, the shape—known as a Koch curve, after Helge von Koch, its inventor—starts to look like a snowflake. And if the transformation is repeated indefinitely, the shape develops some strange characteristics. For one thing, even though it contains a finite area—an area not much bigger than the original triangle—its outline has become infinitely long.

Such shapes seemed intriguing but perverse, clearly figments of the imagination and ostentatiously unlike anything found in nature. The mathematicians who enjoyed constructing such oddities became one side of a gap that emerged between mathematics and the physical sciences.

"They went around patting each other on the back for developing strange constructs outside of nature—they thought they were outsmarting Mother Nature," says Richard F. Voss, an I.B.M. colleague of Mandelbrot's. "What Benoit has done is let some of these monsters out of the closet. They've become the foundation for a new way of looking at the complicated parts of nature."

The mind cannot fully visualize the whole complexity of infinite self-embeddedness. But to someone with a geometer's way of thinking about form, this kind of repetition of structure on finer and finer scales can open a whole world.

"When I came in this game," Mandelbrot says, "there was a total absence of intuition. One had to create an intuition from scratch. Intuition as it was trained by the usual tools—the hand, the pencil and the ruler—found these shapes quite monstrous and pathological."

"Intuition is not something that is given," Mandelbrot says. "I've trained my intuition to accept as obvious shapes which were initially rejected as absurd, and I find everyone else can do the same. These shapes provide a handle to representing nature, and intuition can be changed and refined and modified to include them."

Scientists, no less than builders, work with the tools at hand—and the tools of classical analysis had led mathematicians away from the fanciful shapes that Mandelbrot's imagination ultimately revived.

"The analyst's bag of tricks consists of basically constructing functions," says Mumford at Harvard, "typically solving differential equations that enable you to explore a situation. You would never think of drawing a thing. But with some things, by drawing them you could suddenly get to the heart of the situation."

The drawing tool that makes this exploration possible, of course, is the computer, ideally suited to a kind of picture making that requires millions of repetitions of simple calculations.

When Mandelbrot began his work, he was not alone in examining the powerful notion of self-similarity. The physicists Kenneth G. Wilson, Michael Fisher and Leo Kadanoff did so in developing renormalization group analysis, a rich and highly productive advance that won Wilson the Nobel Prize in 1982. Renormalization is a way of slicing through the mathematical thickets that surround problems involving millions of pieces of matter interacting on scales from the very small to the very large.

"It was an analytical thing for Ken; it enabled him to compute things," Mumford says. "The unique thing in Mandelbrot's point of view was the realization that there was beautiful geometry in it."

Now that Mandelbrot has become a fixture of the scientific lecture circuit, with his indispensable trays of color slides, with his wispy white hair straggling back from his heavy brow—now that he seems to be everywhere, some mathematicians are starting to wonder whether enough isn't enough.

In fact, some of them call him a megalomaniac. "Of course," says Mumford, "he is a bit of a megalomaniac, he has this incredible ego, but it's beautiful stuff he does, so most people let him get away with it."

The business of taking and giving credit can become obsessive in science. Mandelbrot does plenty of both. His book, *The Fractal Geometry of Nature*—his one major work, having gone through several incarnations in several languages—rings with the first person: “I claim . . .” “I conceived and developed . . . and implemented . . .” “I have confirmed . . .” “I show . . .” “I coined . . .” “In my travels through newly opened or newly settled territory,” he writes, “I was often moved to exert the right of naming its landmarks.”

Some scientists don’t appreciate this kind of thing. Nor are they mollified that Mandelbrot is equally copious with his references to predecessors, some thoroughly obscure. They think it’s just his way of trying to position himself squarely in the center, setting himself up as a pope, casting his benedictions from one side of the field to the other.

They also say they resent the way he pops in and out of different disciplines, making his claims and conjectures and leaving the real work of proving them to others. And, for that matter, they don’t like the way he calls to complain about their articles when he feels they haven’t given him enough credit.

“Matters of credit are everywhere,” Mandelbrot says. “And there is a basic unlikelihood of what I have done having been done by one person, which makes people think it’s unlikely so it’s probably untrue. It’s something which is very much part of everyday life in academia, where tempers are strong.”

It hardly matters. The face of genius need not always wear an Einstein’s saintlike mien. But some scientists believe the reaction to Mandelbrot comes from his persistent crossing of disciplinary lines, his refusal to abide by the usual dogmas.

“His kind of work offends a lot of pure mathematicians, because it doesn’t involve the kind of solid proofs that they like to see,” says J. Doyne Farmer, a physicist at Los Alamos National Laboratory. “They get bothered when some guy comes along and does something that is clearly mathematics but not the way that mathematics is normally done—theorem, proof, theorem, proof, theorem, proof.”

“There were a lot of mathematicians going around looking carefully at certain trees that they didn’t think even really existed in the physical world. Mandelbrot said there was a forest there. And he gives a very nice and compelling description of what that forest is and why it’s important.”

For decades, Mandelbrot feels, he had to play games with his work. He had to couch original ideas in terms that would not give offense. He had to delete his

visionary-sounding prefaces to get his articles published. When he wrote the first version of his book, published in French in 1975, he felt he was forced to pretend it contained nothing too startling. That, he says, is why he wrote the latest version explicitly as "a manifesto and a casebook." He was coping with the politics of science.

"The politics affected the style in a sense which I later came to regret," he says. "I was saying, 'It's natural to . . . ' 'It's an interesting observation that . . . ' Now, in fact, it was anything but natural, and the interesting observation was in fact the result of very long investigations and search for proof and self-criticism. It had a philosophical and removed attitude which I felt was necessary to get it accepted. The politics was that, if I said I was proposing a radical departure, that would have been the end of the readers' interest.

"Later on, I got back some such statements, people saying, 'It is natural to observe . . . ' That was not what I had bargained for."

Mandelbrot's attitude toward the scientific establishment, along with his attitude toward established science, has roots in his odd early history. He was born in Warsaw in 1924 to a Lithuanian Jewish family, his father a clothing wholesaler, his mother a dentist. The family moved to Paris in 1936. The war pushed him to Tulle, in south central France. His schooling was, at best, irregular and discontinuous. Even now, Mandelbrot claims not to know the alphabet. Having to use a telephone book, he says, reduces him to near helplessness.

Afterward, at the renowned *École Polytechnique*, he found himself mentally sidestepping mathematics that required a training he never had. He would find roundabout solutions, take geometric shortcuts, transforming the problems into shapes and working the shapes over in his mind. "I could never have done them the straight way," he says. "The system molds people in a certain fashion. I was not affected." When he came to the United States, first to study at California Institute of Technology in 1947, he remained an outsider, and that feeling stayed with him when he first began to bring his ideas about self-similarity to the attention of different fields.

"I don't belong to any of the groups," he says, "and my work flies against the natural tendency of everything to divide itself into pieces." Looking back, Mandelbrot sees his approaches to people in various disciplines as having fallen into sadly predictable stages.

The first stage, as he recalls it, was always the same: Who are you and why are you interested in our field?

Second: How does it relate to what we have been doing, and why don't you explain it on the basis of what we know?

Third: Are you sure it's standard mathematics? (Yes, I'm sure.) Then why don't we know it? (Because it's standard but very obscure.) "Most of mathematics has never been read," Mandelbrot says. "Mathematics is like the delta of a river. It has many branches, some broad and moving rapidly, some narrow and moving little or not at all. In physics, everything which has not worked out has disappeared. In mathematics, people can actually say, 'A problem raised by Eisenstein in 1842 deserves further attention.' Many of the things I have done belong to slow-moving branches."

Fourth: What do people in these branches think about your work? (They don't care, because it doesn't add to the mathematics. In fact, they are surprised that their ideas represent nature.) To reach stages of acceptance and participation, Mandelbrot exploited the uncanny tendency of fractals to turn up in different fields. To economists, some of Mandelbrot's fractal patterns looked indistinguishable from records of stock-market prices. To hydrologists, they looked like historical records of the rise and fall of rivers. By using simple mathematics based on the principle of self-similarity at different scales, and by varying the fractal dimension to mimic more or less violent tendencies to fluctuation, he produced convincing fakes of natural phenomena. Similar techniques, perfected at I.B.M., allow computers to produce astonishingly realistic landscapes—fractal coastlines, fractal mountains, fractal clouds—and they have been adopted wholesale by Hollywood's special-effects industry.

Mandelbrot's mimicking of stock market and river charts does not help in predicting particular rallies and floods. But they have brought some important realizations. Economists needed to understand the heretical idea that prices don't change in a smooth, continuous flow. They can change abruptly, in instantaneous jumps. And dam builders, reservoir builders and risk insurers of all kinds needed to understand that traditional notions of probability were leading them to underestimate the likelihood of the rarest, most catastrophic events.

When a scientific revolution takes place—a thoroughgoing conceptual turnabout with its own lexicon and its own special tools—it may nevertheless leave the culture absolutely cold. But the ideas of fractal geometry, the ideas of chaos, the ideas of what specialists like to call nonlinear dynamics—these notions seem to work as metaphors, too, for the way nonscientists think about the world. Pure mathematicians treat metaphors with justifiable suspicion. But

the recognition of structure amid complexity and randomness, the search for similar patterns at different scales, the willingness to think in terms of discontinuities and leaps, has spread to places where strict mathematics may or may not apply.

These changing ideas arise from a sense of the world that nonscientists share with scientists. No one has to imagine what the universe might be like on microscopic or telescopic scales—microscopes and telescopes make those images part of everyday experience. “Photographs in magazines have brought to the ordinary person things which Leibniz was thinking about in the 17th century,” Mandelbrot says. “Leibniz had no illustrations, he had no tools, the questions he was asking remained abstract.” At the same time, with computers everywhere, it is easier to develop an instinct for the possibilities of simple operations repeated over and over again. Programs to produce simple fractals on home screens have already become a popular staple of computer bulletin-board networks.

To Mandelbrot, with his obstinate fondness for the antique and the obscure, parallels to his geometry are everywhere, in art as much as science. His fractal ideal in architecture would be something like the Paris Opera, brimming with beaux arts complexity, a mixture of orderliness and wildness and—most important—something to hold the eye at any scale, from five feet away or 500 yards. The antifractal ideal, of course, comes from the Bauhaus, all Euclidean simplicity.

“As humans we live in a world with trees and mountains, which have this extreme wealth of structure,” he says. “Structures which are very spare seem unsatisfying.”

In some areas, the appreciation of scaling patterns matters most as a unifying principle. “There is a very subtle question which is quite important to my viewpoint of the world,” Mandelbrot says. “Is the climate different from the ordinary changes in the weather? Are there some mechanisms which rule daily fluctuations, and different mechanisms for yearly fluctuations, droughts and so on?”

The same question applies to economics. Daily fluctuations are treated one way, while the great changes that bring prosperity or depression are thought to belong to a different order of things.

“In each case,” Mandelbrot says, “my attitude is, let’s see what’s different from the point of view of geometry. What comes out all seems to fall on a continuum—the mechanisms don’t seem to be different.”

Surely droughts and depressions have real causes, physical and political causes. But the claim of fractal geometry is that those causes, whatever they are, belong to the same universe that controls events at much finer scales.

Graphic computer representations of some simple fractals look so real—so alive—that they sometimes seem like parlor tricks. At I.B.M., Richard Voss creates moss, seaweed, roots. “How can something with such simple rules produce structures that look so alive?” he asks. There is no answer, except a hopeful suspicion that this new mathematics has hit upon a fundamental organizing principle of nature. Perhaps laws of adaptation and economies of genetic coding tend to stay in certain paths. These are notions just beginning to be explored.

“The questions the field attacks are questions people ask themselves,” Mandelbrot says. “They are questions children ask. What shape is a mountain? Why is a cloud the way it is? People want to describe this universe, this reality, which is so very fugitive.”

December 8, 1985

Snowflake's Riddle Yields to Probing of Science

By JAMES GLEICK

Science has conquered the snowflake problem.

In resolving two of nature's most poetic and maddening riddles—why are snowflakes symmetrical, and why are they all different—theoretical physicists have created a new body of mathematics for the laws that control the delicate branching growth of an unstable solidifying crystal.

Where traditionally snowflakes were left to weather experts and atmospheric scientists, now they have become part of a growing science of pattern formation that is drawing together theorists, computer modelers and engineers with practical problems ranging from metallurgy to flame propagation to oil recovery. The principles that govern ice crystals apply as well to metallic crystals, whose microscopic structure helps determine the strength of cast alloys.

Generations of snowflake-watchers sketched and catalogued the variegated patterns formed by airborne ice crystals: plates and columns, crystals and polycrystals, needles and dendrites. But snowflakes obey mathematical laws of surprising subtlety, and it has been impossible to predict precisely how fast a tip will grow, how narrow it will be or how often it will branch.

"In the last two years, those problems have been solved," said Herbert Levine of the Schlumberger-Doll Research Center in Connecticut, one of the pioneers of pattern-formation research. The most recent breakthrough has provided a working mathematics for tying together the forces that stabilize the growing patterns and the forces that destabilize them.

By understanding the interplay of randomness and determinism, large-scale processes and microscopic processes, this new wing of physics has related a variety of subjects that were formerly treated separately.

"We've reached a very interesting point scientifically where we're starting to look at a whole bunch of older problems of pattern formation in nature, how complex formations emerge out of a generally featureless soup," said James S. Langer of the Institute for Theoretical Physics in Santa Barbara, Calif. "We finally seem to have a good idea of what controls these things."

A key to the new approach has been the availability of computers with which scientists could propose models, test them, make pictures of the results and then

improve their models. Only recently, though, after more than five years of research by several groups, have computer simulations succeeded in realistically capturing the physics of crystal growth.

One problem is that such growth entails, as Dr. Langer says, "a highly non-linear unstable free boundary problem," meaning that models need to track a complex, wiggly boundary that changes dynamically. "That's tough, trying to understand where this boundary is moving," he said. "If you guess wrong, the computer program just blows up on you."

Another problem has been deciding which of the many physical forces involved are important and which can safely be ignored. Most important, as scientists have long realized, is the diffusion of the heat released when water freezes.

When solidification proceeds from outside to inside, as in an ice tray, the boundary between solid and liquid generally remains stable and smooth, at a speed controlled by the ability of the walls to draw away the heat. But when a crystal solidifies outward from an initial seed—as a snowflake does, grabbing water molecules while it falls through the moist air—the process becomes unstable.

Any bit of boundary that gets out ahead of its neighbors gains an advantage in picking up new water molecules and therefore grows that much faster—the "lightning-rod effect." Tips, or "dendrites," form, moving rapidly outward and tending to give birth to subbranches.

This much has been known for years. But the physics of heat diffusion and unstable growth cannot completely explain the patterns scientists observe when they look at snowflakes under microscopes or grow them in the laboratory. Recently Dr. Langer's group in California and Dr. Levine's in Connecticut separately worked out a way to incorporate another process: surface tension.

Where diffusion creates instability, surface tension creates stability, preferring smooth boundaries like the wall of a soap bubble. It costs energy to make surfaces that are rough. And where diffusion is mainly a large-scale, macroscopic process, surface tension is strongest at the microscopic scales.

The competition between these forces makes for tricky mathematics, particularly since the equations must relate scales of millimeters to scales of molecules. Traditionally, physicists assumed that for practical purposes they could disregard the tiny surface-tension effects.

"That turned out to be just wrong," Dr. Levine said. "The breakthrough was showing that by throwing away this particular physical effect one was throwing away the right solution to the problem."

The reason is that the surface effects prove much more sensitive to the molecular crystal structure of a solidifying substance—in the case of ice, a natural hexagonal configuration. That gives ice a built-in preference for six directions of growth.

To their surprise, the physicists found that the delicate balancing act of stability and instability amplifies this microscopic preference, creating the magnificent lacework characteristic of snowflakes.

In effect, a snowflake records the history of all the changing weather conditions it has experienced. As a growing flake falls to earth, typically floating in the wind for an hour or more, the choices made by the branching tips at any instant depend sensitively on such things as the temperature, the humidity and the presence of impurities in the atmosphere.

The nature of turbulent air is such that any pair of snowflakes will follow very different paths, and enough combinations of patterns are possible to more than justify the folklore that all snowflakes are different. But why are all six arms of a snowflake alike?

"Lots of people have thought that there has to be some mechanical equivalent of somebody sitting at the center of the snowflake and telling all of them to do the same thing," Dr. Langer said.

But first of all, careful examination shows that snowflakes are not exactly symmetrical. And second, the six arms of one snowflake, less than a millimeter across, will have experienced nearly identical growing conditions—much closer than any two snowflakes experience, and close enough to explain their similarity.

In metallurgy, specialists seek a precise understanding of what controls the speed of crystal growth and the degree of irregularity because these, in turn, often control the tensile strength of an alloy after it solidifies. These scientists are also benefiting from the new style of using computer models to study such problems.

"There's a brand new interaction between technology and science, connected largely by the computer," Dr. Langer said. "People in industry say, 'We're dealing with more and more complex systems, and we're not going to do it by hunt-and-find any more—it's too tough.'"

Meanwhile, physics groups at École Normale Supérieure in Paris and California Institute of Technology in Pasadena are pursuing the new approach to pattern formation, and a physicist at Emory University in Atlanta, Fereydoon Family, has used the mathematics to create startlingly lifelike computer pictures of snowflakes.

One computer snowflake, an aggregation of 10,000 or more particles, requires about eight hours of high-speed calculation, and very slight changes in temperature or humidity produce vivid changes in the resulting patterns, Dr. Family said. He will present the results at the March meeting of the American Physical Society in New York.

Experimentalists, too, are pushing the science of pattern formation forward. Jerry P. Gollub, a physicist at Haverford College and the University of Pennsylvania, has conducted a series of experiments designed to shed light on the precise shape of the convoluted structures that appear behind the growing tip of a dendrite, a problem that continues to elude theorists.

Using a microscope and crystals of ammonium bromide, he has been able to resolve details as small as 500 angstroms, or $1/20$ th the width of a human hair. Most recently he has been able to characterize the irregularities within rows of these sprouting side branches.

In the back of their minds, many of these physicists nurse a belief that their work on pattern formation may apply to developmental biology as well. Some types of algae, for example, closely resemble patterns under investigation by physicists.

"There is a clear connection between this problem of stability and the early differentiation of certain organisms when they start from an egg and gradually acquire structure," Dr. Gollub said. "What we're really doing is pushing science in a new direction through a simultaneous development in mathematics and experiment.

"On the one hand snowflakes are important because there are lots of crystals in nature," he said, "but in the long run I think the most important aspect will be this general development of tools and ways of thinking. It is those things that are most likely to carry over into other areas of investigation."

January 6, 1987

Tales of Chaos: Tumbling Moons and Unstable Asteroids

By JAMES GLEICK

Bad news for those who thought they could at least rely on the stable clockwork predictability of heavenly bodies: the solar system has some surprises in store.

A new picture of celestial motion suggests that the earth's neighbors include erratically tumbling moons and unstably orbiting asteroids, a chaotic menagerie that seems to provide, among other things, a solution to the longtime mystery of where meteorites come from.

"We have a strong prejudice that the solar system is dull—perhaps pretty, but not very interesting dynamically," Jack Wisdom of the Massachusetts Institute of Technology told an audience of physicists, mathematicians, chemists and biologists here this week. In fact, he said, the solar system's spins and orbits are neither so simple or so regular as Newton's descendants might expect.

New computer calculations, based on observations from the Voyager satellites and ground-based telescopes, show that just about every moon—except the earth's—has experienced millions of years chaotic tumbling, Dr. Wisdom reported. As he showed with a computer-generated movie, "tumbling" is a kind of motion utterly unlike the familiar spin of a body around an axis.

A tumbling moon falls end over end, twists sidewise, speeds up, slows down, all the time obeying Newton's completely deterministic laws of motion, yet defying prediction in a way that scientists used to consider impossible. One of Saturn's moons, a 250-mile-long football-shaped body called Hyperion, appears to be tumbling now, and its unpredictability is such that even if Voyager I had measured Hyperion's position and speed to 10-digit accuracy, God's own computer would not have been able to calculate where it would be when Voyager II came by a year later.

Hyperion is not alone, according to Dr. Wisdom's latest work. The moons of Mars, Phobos and Deimos, went through tumbling episodes on the order of tens of millions of years, and the propensity to tumble is the rule, not the exception.

Strangely, tumbling results from precisely the same gravitational laws and tidal forces that cause moons to lock into a stable orbital "resonance" with their

planets. The earth's moon spins once for every orbit, thus always showing the same face. Nor must the ratio be one to one. Mercury, for example, was long thought to keep the same face pointed to the sun; in fact it rotates exactly three times in every two of its "years."

Such resonances are not permanent, because energy drains away, lost to tidal friction. And when a moon breaks out of a locked mode, tumbling can ensue. The lesson for science—and it has been a hard lesson even for physicists to grasp—is that chaotic behavior is just the flip side of a simple Newtonian coin.

"Here is a departure from everything you've expected," said James Yorke, a mathematician from the University of Maryland. "You have no special perturbation or complexity. It's just basic physics—yet it's doing something that nobody thought about."

This was Chaos '87, a conference subtitled "The Physics of Chaos and Systems Far from Equilibrium" and attended by theorists and experimenters from 14 countries, including China and India. "We're the revolutionaries plotting to bring order into chaos," David Campbell of Los Alamos National Laboratory told his colleagues.

The scientists belong to a rapidly growing interdisciplinary field devoted to complex dynamical behavior in systems from astronomy to biology. They presented new results on the fantastic structures that arise in crystal growth and on the bizarre palm tree-like formations of intense shock waves. They described highly sensitive experiments designed to tackle the problem of tumult in fluid flows. One biologist promised a chaos approach to the problem of sexual reproduction, but ran out of time.

As some saw it, the latest results suggest progress in moving beyond "simple chaos" to more complex systems—for example, in one version of the jargon, beyond "wimpy turbulence" to "macho turbulence." At any rate, they argued, the era of simple, linear mathematics is over. "Ideal problems are just in the textbooks, for the joy or desperation of students," said F. Tito Arcelli, a laser physicist from Istituto Nazionale di Ottica in Florence.

A new theoretical approach to fluid turbulence came from Steven A. Orszag of Princeton University who also showed his audience a slide depicting a newspaper advertisement for the Off Broadway play *A Girl's Guide to Chaos*, described as a belly full of laughs and a glorious gigglefest.

"I hope these views of chaos don't apply here," Dr. Orszag said. He need not have worried.

As is customary at high-level conferences, speakers did not always pitch their talks to the broadest possible segment of their hundreds of listeners. Mitchell J. Feigenbaum of Rockefeller University, whose theoretical breakthroughs in the 1970s gave strong impetus to the study of chaos, was one of several speakers who presented dazzling exercises in mathematical physics, greeted by a presumably respectful silence.

Did Dr. Feigenbaum feel that his presentation was understood? "Certainly," he said. "I'm sure Yves Pomeau understood it," he said, referring to a theorist from École Normale Supérieure in Paris. "And I know Tito Arecchi understood it, because he's heard part of it before."

A key to the progress in chaos—both cause and consequence—is the ubiquity of computers. James Glimm, a mathematician from New York University's Courant Institute, studying a variety of "things that wrap around and get mixed up and entangled with one another," went so far as to say that there are now three ways of doing science.

"There used to be two: theory and experiment," he said. "Now we have computing as well." And it was computing that enabled Dr. Wisdom of M.I.T. to solve the meteorite mystery.

Astronomers have long suspected that meteorites striking the earth were stragglers from the asteroid belt, the vast region between Mars and Jupiter filled with flotsam and jetsam. Other sources were proposed—comets, for example—but the asteroid belt has the most obvious abundance of suitable material.

The problem is, if meteorites are wayward asteroids, how do they get from there to here?

Some scientists proposed asteroid collisions as a mechanism. But to change an asteroid's orbit enough to send it all the way to earth, a collision would have to cause a change in speed of well over 10,000 miles an hour. Any collision capable of imparting that much energy would smash an asteroid into oblivion.

"It just doesn't work," said George Wetherill of the Carnegie Institution in Washington, an authority on the solar system who suggested the problem to Dr. Wisdom. "You need a gentle gravitational mechanism."

Dr. Wisdom, meanwhile, was thinking about a different problem, the "Kirkwood gaps" in the asteroid belts. Astronomers have known for a century that asteroids with certain orbital periods were strangely sparse.

It happens that the missing asteroids are the ones that would have certain resonances with the orbiter of Jupiter, such as 3 to 1, 5 to 2 and 7 to 3. So some

theorists speculated that the periodic gravitational kick of Jupiter might account for the missing asteroids, but calculations failed to demonstrate this idea. On the contrary—in the long run, it seemed, asteroid orbits should remain stable.

But Dr. Wisdom, using new mathematical techniques and a special-purpose celestial mechanics computer, built for him by an M.I.T. colleague, has solved both problems at once. Over very long time scales, when the perturbing influences of both Jupiter and Saturn are taken into account, the seemingly regular orbits of asteroids that stray into the Kirkwood gaps turn chaotic.

For millions of years, he found, such an orbit seems predictable. Then the path grows increasingly eccentric until it begins to cross the orbit of Mars and then Earth. Collisions or close encounters with those planets are inevitable.

To many astronomers, such chaotic “bursts” of eccentricity seemed implausible. “When Wisdom showed you could get this chaotic effect, it was met with considerable skepticism,” Dr. Wetherill said. “There was a tendency among almost everybody to say, ‘Well, he just doesn’t know how to integrate yet, wait till he gets a little older, he’ll understand these things.’”

But most are now convinced. Among other things, his trajectories correspond to a quirky piece of meteorite lore known as the afternoon effect: the tendency of meteorites to fall most heavily in the afternoon. As it happens, afternoon is when any part of the earth is facing the right way to capture misguided asteroids.

“It’s sort of fun to see the true harmonies of the spheres here,” Dr. Wisdom says. His next project is Saturn’s rings, and he is also carrying out intensive calculations to check whether the solar system as a whole is stable or whether the planets will eventually go chaotic themselves.

It is an open question, but so far, he said, the solar system seems stable.

January 20, 1987

Fluid Math Made Simple—Sort Of

By JAMES GLEICK

Of all the hard problems occupying the world's supercomputers, one heads the list: calculating the flow of fluids.

The equations that engineers use to study how air flows past the wing of an aircraft or water around a ship's hull are notoriously hard to solve, straining even the most powerful computers. Yet these kinds of calculations pop up again and again, not only in designing planes, ships, rockets and automobiles but in forecasting the weather, which is one of the most difficult fluid-flow problems of them all.

For the last few decades, computer scientists have tried to extend their grasp of such problems by designing ever more powerful computers, like the Cray-2 recently dedicated by the National Aeronautics and Space Administration at the Ames Research Center in Mountain View, Calif. But even it is inadequate. What is needed, some physicists have come to believe, is a radically new approach to mathematical modeling, the method by which computers are used to simulate and predict the phenomena of the world.

Guided by this vision, a strange new wing of theoretical physics has found a way to sidestep completely the calculations that computers find so fiendish. Instead of using complex equations to mirror fluid flow, physicists are creating fantastically simple mathematical models known as cellular automata.

A cellular automaton is a large array of cells, like the squares of a checkerboard or the hexagons of a honeycomb, which can be projected onto a computer screen. On this lattice, dots hop from cell to cell, colliding and recoiling according to a few simple rules programmed into the computer. From millions of these minute interactions, a picture emerges of such familiar physical phenomena as the pattern water takes when it flows past a rock in a stream.

These models, which are called automata because they run according to their own rules of motion, provide physicists with a miniature simulation of the universe. In the real world, space and time are continuous, or so physicists assume. In the simplified world of cellular automata, space is represented by the grid of cells. In the real world, molecules can move freely in infinitely many directions, at infinitely many speeds. In cellular automata, the dots are allowed to occupy only the cells of the lattice and can travel at only one speed.

By imposing so many constraints, these models seem at first to sacrifice the richness of the real world. But they gain in return an astonishing improvement in the speed of calculation. And to the surprise of some physicists, they seem to work.

"We're realizing that we don't need all these details that we've been worrying about all these years," said Brosl Hasslacher, a physicist at Los Alamos National Laboratory. "The reason people are super excited is that these skeletal micro-worlds, which completely eliminate the details of real fluids, capture everything. I think we've just begun to see the power of it."

American and French researchers say the new models are especially useful for calculating flows around complicated shapes, like the rear-view mirrors on the sides of a car. In a standard supercomputer, such shapes require many numbers to describe, making the calculations extremely complex. In cellular automata, shapes can simply be drawn onto the grid with a computer graphics terminal.

Because the same simple calculations are repeated millions of times, cellular automata are especially well suited to a new breed of computers that perform parallel processing. Even the powerful Cray supercomputers are essentially serial machines: they break a problem into thousands of pieces that must be funneled one at a time through a large central processor. Parallel machines avoid this bottleneck by using many processors to solve many pieces of a problem simultaneously.

The idea of using cellular automata to simulate fluids is new, but the models go back to John von Neumann, who in the 1940s was one of the founders of computer science. Recently several theorists, most notably Stephen Wolfram, director of the new Center for Complex Systems Research at the University of Illinois, and Tommaso Toffoli at the Massachusetts Institute of Technology, have turned to these simplified models as a way of studying a variety of fundamental questions in physics.

"You're playing God's game," said Dr. Toffoli, whose group has built machines designed especially for cellular automata. "What you have essentially is a universe synthesizer: You give the laws, the rules of the game."

The rules can be adjusted for many sorts of problems. At the Illinois center, Norman H. Packard has designed cellular automata in which the tiny dots interact to generate the kaleidoscopic patterns typical of the formation of snowflakes and other crystals.

For some scientists, this communication across scales, from the small and simple to the large and complex, gives cellular automata their deepest charm.

"I find it fantastic and beautiful that the tiny, trivial world of the lattice gas can give rise to the intricate structures of hydrodynamic flow," Leo Kadanoff of the University of Chicago wrote in *Physics Today*. "The physical universe is also wonderfully simple at some levels, but overpoweringly rich in others."

April 19, 1987

When Chaos Rules the Market

By JAMES GLEICK

That the stock market embodies turbulence, mayhem and unpredictability, no survivor of October 1987 can doubt. Some economists, borrowing the vocabulary of a new branch of science, now believe that it also represents chaos.

The science of chaos—a fast-growing, interdisciplinary exploration of complex systems from the weather to the human heart—has challenged conventional approaches to random-seeming phenomena, offering innovative techniques for unraveling disorder. Economists are beginning to apply those techniques to the especially intricate and self-conscious brand of disorder displayed by the financial markets. In the aftermath of the explosive movements of the last month, some researchers believe that the methods of chaos theory may be particularly appropriate to the stock market, a system famous for creating trends and patterns and then violently defying them.

As applied to economics, a notoriously fickle science, such ideas are uncertain and untested. Nevertheless, for those who follow the market closely, they offer a new way of looking at familiar problems, from the market's internal workings—the intricate web of trading that runs from brokerage computers to the floors of the exchanges—to the overarching forces of the world's economy.

"We now know very clearly that stock market prices cannot be analyzed by the old procedures that we used," said James Ramsey, a New York University economist who has become a specialist in chaos. "People are asking more cogent questions, and they're observing behavior that begins to be amenable to the ideas of chaotic dynamics."

The stock market is the economy's most visible showplace for the waxing and waning of wealth and confidence—a sensitive hybrid of the facts of corporate finance and the whims of mass psychology—and even the relatively unorthodox economists who have been thinking about chaos disagree about just how their new ideas apply. Nevertheless, they are already engaging in some provocative speculation:

- * Some contend that the market may be becoming unbalanced as information flows more efficiently and as traders grow more sophisticated in responding to it. As the global network of buying and selling

becomes increasingly interconnected and computerized, they suggest, it may be leading to volatility of a kind never before seen.

- * Others suggest that chaotic leaps in prices undermine some key techniques for hedging against loss, requiring a reassessment of traditional market safeguards. Chaos theory cannot help in predicting stock prices, they say, but it may help guide those who make the rules by which the game is played.
- * Chaos theory provides a more subtle way of thinking about the effects of global forces like the budget deficit and the balance of trade. Such effects, the researchers say, can interact in unexpected ways, with time lags that sometimes obscure their importance.
- * Traditional ways of looking at stock market data, from random walk theory to technical analysis, come into serious question in light of chaos, according to some economists.

Extreme events—unexpectedly fast and unexpectedly large—are a hallmark of chaotic systems. Physicists have learned to focus on the way tiny fluctuations are magnified, turning small bits of instability into large-scale booms and busts. Some scientists believe that the stormy oscillations of the last month reflect those tendencies in the financial markets.

“Somebody who’s worked on chaos is in no way surprised that this sort of thing happened,” said David Pines, a University of Illinois physicist. “It’s expected of such systems—they’re so sensitive to small perturbations.” Dr. Pines helped organize a meeting of leading economists and chaos theorists at the Santa Fe Institute in New Mexico to explore such possibilities in September, “pre-Black Monday,” he said.

When they speak of chaos, scientists mean erratic behavior that appears to be random but is not. The essence of their approach is a search for underlying patterns of a kind that have been discovered in a wide variety of seemingly random systems. Scientists studying chemical reactions, wildlife populations and electronic circuits have found that surprisingly simple systems can produce streams of data that rise and fall as erratically as the stock market, indicating that they may be governed by the rules of chaos.

But unlike any physical system, economics exists in a world with politics and history. It has the doubly entangled complexity that comes with human behavior: the same people who are trying to understand the stock market are quite capable

of influencing the variables they seek to predict.

"Economic models are filled with agents that are trying to understand what other agents are doing, unlike physical models," said William A. Brock, a University of Wisconsin economist. Weather forecasters, essentially unsuccessful at predicting their version of chaos, at least know that the laws of physics remain unchanged from day to day and that cyclones and anticyclones will not suddenly develop will and memory.

Still, some economists familiar with the details of modern trading technologies believe that chaos theory gives a telling look at forces of instability that tended to elude older models of economic behavior. Because traditional methods were geared to understanding such concepts as equilibrium, economists tended to focus on the forces of order. "Before nonlinear dynamics started capturing people's imagination, we basically spent most of our time on evidence of stability," Dr. Brock said.

Global Instability

There were moments, during the frenzied collapse of Oct. 19, when the stock market produced the financial equivalent of water flowing uphill.

Options to buy or sell stock—calls and puts—were seen moving in precisely the wrong direction, as the usual computer-controlled relationships broke down in the face of the rapid swings. And stock prices leaped across broad gaps, frustrating strategies meant to insure against less extraordinary declines.

The wildness offered a vivid example of how large-scale behavior emerges from the microscopic details of trading. As prices began to plummet, the market turmoil did not seem directly tied to the grand trends of budget deficits or the psychology of world events. Though analysts have tried, none have found a convincing trigger for the collapse in the Capitol or the Persian Gulf.

The real dynamics of the collapse were such contingencies as whether an over-the-counter market maker could or would answer his phone at a given instant; whether a sharp price change would breach a threshold and set off computers managing the intricately timed strategies of program trading and portfolio insurance; whether a simultaneous order to buy or sell the 500 individual stocks that compose a Standard and Poor's index could be handled by the frantic specialists on the market floor.

Whether the mechanics of such events can be convincingly modeled by the techniques of chaos, or "nonlinear" dynamics, is far from clear. Physics and

mathematics do not offer simple equations for human turmoil.

"It is true that people who have been studying the stock market with the tools of nonlinear dynamics have found, before this last episode, evidence of chaotic behavior," said Kenneth J. Arrow, a Stanford University economist and Nobel laureate. "It's tempting to jump from that to a statement about recent events, but I don't think anything can explain a fall of 20 percent in one day."

Nevertheless, some economists contend that chaos provides a natural way of seeing the crucial connections between the details of trading and the large-scale dynamics of the market.

The economy, like complex systems in nature, combines forces on the microscopic scale and the global scale. Just as the observable behavior of the earth's atmosphere emerges from the interaction of a nearly infinite number of molecules, large-scale movements in the financial markets arise from millions of individual decisions to buy and sell.

In chaotic systems, surprises occur when the individual components are added together. In the stock market, one surprise that traders and market officials continue to debate fiercely has been the combined effect of powerful new techniques like program trading, the computer-managed arbitrage of index futures. Some chaos theorists believe that such trading is only a piece of a larger, possibly foreboding picture.

Program traders make money from small discrepancies that appear between the prices of index futures and the underlying stocks. One force that creates such discrepancies is portfolio insurance, a method of hedging against loss that led, on Black Monday, to a sudden and rapid selling of futures.

Index futures allow traders to bet on the mass movements of 100 or 500 stocks; when the price of the futures departs from the prices of the underlying stocks, it is possible to profit by selling one and buying the other. The strategy only works because computers can quickly calculate the small fluctuations and issue hundreds of simultaneous orders.

The consequences are intensely disputed. Program traders, and many economists, argue that such practices make the market more efficient and therefore more stable, by keeping prices in line and preventing large anomalies from opening up. Others contend that the huge volume of buying and selling contributes to volatility.

Program trading was halted after Black Monday and is now resuming, though not yet on its previous scale. Some chaos-minded economists now argue

that whether or not program trading survives, it is only a part of a deeper trend.

They speak in terms of information flow and the global coordination of market strategies. More than ever, they note, separate markets are working in concert: the stock, credit and currency markets; and the New York, London and Tokyo markets.

Inefficiency, they suggest, helped keep markets stable. "When no one knows what's going on, or rather everyone has a different opinion, it's like a bunch of atoms bouncing around in a bowl," Dr. Ramsey said. "You get a whole continuum and prices tend to remain in a steady state. So when information comes in, things tend to move very slowly."

When opinions become more harmonious, and reactions become similar, he said, market balance becomes more precarious. If the market turns down for some outside reason, he added, many participants react uniformly—a process of which program trading is a part.

"As we get to more and more uniformity of opinion and more and more uniformity of action, in the sense that people are all following the same rules and the same procedures and using the same data base," Dr. Ramsey said, "then the volatility of the market increases dramatically."

Jagged Edges

Speed of price changes is one issue. The character of those changes—smooth or jagged, continuous or discontinuous—is another.

A few economists believe that another lesson of chaos was confirmed in the minute-to-minute drama of the Oct. 19 collapse: that prices change discontinuously, in jagged steps, rather than the unbroken trajectories that economists traditionally visualize.

The difference is not just academic, as many traders and portfolio managers discovered. When prices leap from one level to another without passing through the intervening points, they can defeat a set of fail-safe strategies based on the traditional assumptions.

"Most traders do tend to think of these things as being continuous," said James L. Kaplan, a Boston money manager with a background in the mathematics of chaos. "Moreover, in their minds, they basically try to fit lines or curves to everything. If you believe the chaotic model, then there's no reason to think that that works."

Many of the complex strategies for protecting portfolios against loss rely on

the ability to buy or sell a stock or a stock option at a certain price. If prices leap discontinuously, those strategies can fail just when they are most needed. Such leaps were witnessed repeatedly on Oct. 19.

"I believe that the most important characteristic of prices is that they can and do change discontinuously fairly often," said Benoit Mandelbrot of the International Business Machines Corporation, who created the branch of mathematics known as fractal geometry.

The assumption of smooth motion is tempting, by analogy with motion in the physical world. But unlike a falling rock, driven by gravity, a stock price is an abstraction driven by the minds of market participants, and minds can change instantaneously.

Specialists who control the setting of prices for individual stocks are obliged to maintain the appearance of continuity, even when it is little more than appearance. When a price leaps from one level to another, specialists often make low-volume trades at the intermediate levels. When the market collapses as quickly as last month, such practices become impossible.

"The principal characteristic of prices in a competitive market of the kind that Wall Street is—and even the ideal Wall Street would be the same thing—is that price is different from all the physical quantities that vary continuously," Dr. Mandelbrot said.

"There is no bound to the amount that prices can jump, as we saw last month."

Fickle Forces

The attention to market dynamics comes amid continuing confusion over the role of national policy and other fundamental forces in influencing the market's behavior. The budget deficit, the dollar's plunge, the inflation rate—such forces certainly affect the market's dynamics, but their effects remain unpredictable. Economists repeatedly find themselves unable to distinguish good news from bad.

Unpredictable, however, does not necessarily mean random. Lessons learned in physics and mathematics over the past two decades suggest a new way of thinking about such forces. Their relationships cannot be graphed with neatly proportional straight lines that correspond to linear equations. They require non-linear equations, which more accurately reflect the interplay of economic forces, but are much harder to solve.

And because nonlinear relationships produce surprising behavior, both their direction and their timing can run counter to ordinary intuition. One of the few near certainties that have emerged in the minds of market analysts and government budget negotiators in Washington is the harmful influence of the federal deficit. The puzzle, as many economists have noted, is that until last month the unprecedented growth of that same deficit ran hand in hand with an ebullient bull market.

Other fundamental elements of the economy are even more confusing. The falling value of the dollar overseas surely plays a key role, yet on any given day, analysts cannot agree on whether the stock market has rallied because of, or in spite of, a rally in the currency markets. Rising interest rates are known to mean falling stock prices—except when, as during the last month, falling stock prices mean falling interest rates.

These and dozens of other important quantities in the global economy are linked to one another like the ligaments, joints and tendons of some improbably entangled anatomy. A push in one place shows up as a nudge or a flutter in many others.

The relationships are mercurial, however, impossible to pin down precisely. That is one symptom of nonlinearity; another is that the relationships are often circular, letting different trends start a chain of events that eventually leads to a kind of feedback.

So falling interest rates discourage foreign investment in American credit markets; an outbound flow of foreign money weakens the dollar; a cheap dollar encourages foreign investment. Or, a cheap dollar encourages exports; increased exports improve the balance of trade; a stronger balance of trade strengthens the dollar.

Economic theorists—if not the practitioners who actually make forecasts and design trading strategies—have recognized the nonlinearity of such systems for some time. Nevertheless, the preferred models of economics have traditionally been linear, meaning that they tend naturally to seek a balanced equilibrium or follow regular, periodic cycles. Those model behaviors, many now feel, are misleading. Chaos theory offers a radically new way of working systems of nonlinear equations and discovering the deeper patterns that often underlie them.

For economists, turning to the methods of chaos has required an uneasy shift in style. Dr. Ramsey, for example, deliberated carefully before making the shift, worrying at first that such unorthodox ideas might jeopardize his reputation. He now actively advocates an interdisciplinary approach.

Others, like Dr. Arrow, are cautious but intrigued. Dr. Arrow has long been a leading economic theorist, putting forward ideas that trickle down only slowly to

actual market practitioners, and, along with Dr. Pines, he was an important force behind the meeting in Santa Fe.

The meeting brought together experimental physicists and computer modelers, who described their success with chaotic models of natural systems. Many economists who participated said that they had begun to see the limits of more orderly models based on old ideas about how systems come to equilibrium.

"They've really recognized that what they're doing isn't working, but they haven't seen a better way to go," Dr. Pines said. "What's missing is the notion that things might really be chaotic, not orderly, and that these interactions can lead to genuine instability."

A powerful tradition in stock-watching has treated price fluctuations as purely random—a "random walk," as one school has it. The market has no memory, according to extreme forms of the random-walk view; its ups and downs on any given day bear no relationship to previous moves—or to real economic trends.

Not-So-Random Walk

Some of those who favor chaos assert that the scale of last month's collapse was too vast to be explained as part of a random walk.

"The random-walk approach says there is no underlying dynamic," said James A. Yorke, a mathematician who is acting director of the Institute for Physical Science and Technology at the University of Maryland. "I think the drop on Black Monday is inconsistent with the random-walk approach. If you look at the size of fluctuations on a typical day, there's essentially no probability of a drop of 500 points."

Other chaos specialists contend that random-walk theory is equally helpless in explaining longer trends like the strong run-up in the stock market early this year. Such trends show that an effective model must have some memory of past behavior, they said. In any case, the chaos approach prefers not to fall back on unexplained randomness.

Chaos "poses some real dilemmas for economic theory," said Dr. Arrow of Stanford. "It creates the idea that you have a mechanism which produces cycles, produces amplified fluctuations and doesn't depend on accidents, the way random walk theory seems to do."

Thus, real causes and effects do govern market behavior. But in nonlinear models, their workings are not always easy to discern. Population biologists and

epidemiologists, for example, know that as an epidemic courses through a real population, the number of victims often fluctuates erratically. To gain insight into such behavior, they devise mathematical models meant to mimic real life. To their surprise, they have found that the simplest of models, as long as they are nonlinear, can produce wild fluctuations.

One revealing approach is watch how such models behave when altered by a sudden jolt of some kind. Robert May, an influential Princeton University biologist, has described the surprising behavior of a simple model for the yearly progress of a disease. When the model is "perturbed" by a change responding to a program of inoculation, the level of disease does not coast downward smoothly, as traditional epidemiologists might expect.

Instead, the model embarks on a series of broad oscillations, swinging downward one year but up again the next. Only after several years have passed does a new, healthier equilibrium emerge. In real life, similar patterns have been observed.

A policy maker seeing an upward swing might be tempted to look for a specific cause of the disease's resurgence, not realizing that such oscillations are a natural, predictable outcome of a nonlinear system. Similarly, chaos theorists suggest that the stock market's behavior does reflect underlying economic forces—but with time lags and patterns of oscillation that remain inscrutable.

"In all nonlinear processes that I've ever looked at, there are always large excursions," said Henry Abarbanel, a physicist who heads the Institute for Nonlinear Science at the University of California at San Diego. "They don't represent major instabilities in the system; they simply represent the fact that you can concentrate energy or momentum or whatever is the appropriate dynamical variable. That's what I think is happening." Such methods are most successful in helping understand the general character of irregular behavior—the degree of volatility or the likelihood of oscillations. They can help in predicting how changes in a system's rules might increase or decrease stability.

Whether they will ever help economists make more precise predictions remains in question. For now, many economists believe it will be hard enough for their science to become comfortable with extreme and extraordinary occurrences—events that used to be treated as exceptions. Psychologically, that remains difficult, as those studying chaos have discovered.

"The phenomenon of extreme events being viewed as being individual acts of God, as opposed to daily ordinary behavior," Dr. Mandelbrot said, "is one that is very natural to the human race."

The Right Way and the Wrong Way

When it comes to choosing the right way to look at stock market data, chaos theorists are nearly as contentious as other economists. When it comes to the wrong way, however, agreement is easier to come by. These are some common statistical tools and tricks that, by the lights of chaos, seem hopelessly naive:

- * Smoothing out the bumps. A variety of techniques, such as “moving averages,” are meant to eliminate fluctuations in series of data, in hopes that elements of randomness can be separated from the real information. To a scientist who has studied chaos, trying to make smooth curves out of jagged data is a mistake—the volatility is just as real as the average, and just as important in puzzling out the underlying dynamics.
- * Juxtaposing separate data. Analysts often try to line up a chart of the value of the yen, say, or the monthly trade deficit, with a chart of stock market prices over the same period, hoping to discern a visual similarity. Such artificial parallels are almost always illusions, chaos theorists say. The real connections between such factors are far more complex, usually involving variable time lags.
- * Forecasting by cycles. Although the human eye is extremely adept at picking regular cycles out of data series, those, too, are optical illusions. Real cycles in chaotic systems are almost never truly periodic. That is why, when analysts purport to see cycles of every 3 years, or every 20 years, or every 9½ months, the cycles are not likely to come around on schedule next time.
- * Forecasting by “chartism.” Chartists and other technical analysts go beyond cycles in search of more arcane patterns—the “head and shoulders” or the “three peaks followed by a house.” Although chaos theorists do try to find the patterns hidden in price data, the analysis is far more complicated. Mathematicians have firmly established that specific long-term predictions in a chaotic system cannot be made on the basis of past ups and downs.

November 22, 1987

New Appreciation of the Complexity in a Flock of Birds

By JAMES GLEICK

Nothing in the motion of a single bird or a single fish, no matter how graceful, can prepare a scientist for the sight of 10,000 starlings wheeling in formation over a cornfield, or a million minnows, threatened by a predator, snapping into a tight, polarized array.

Yet somehow the actions of individual animals sum together in ways that researchers are only beginning to understand, creating patterns of motion so complex that they seem to have been choreographed from above. Flocks and schools have a distinctive style of behavior—with a fluidity and a seeming intelligence that far transcends the abilities of their members.

Vast congregations of birds, for example, are capable of turning sharply and suddenly en masse, always avoiding collisions within the flock, and zoologists now believe that such movements take place without guidance from a leader. Fish, too—their vision limited in murky seas—manage complex, seemingly instantaneous maneuvers when alarmed by an intruder.

Flocking and schooling create some of life's most breathtaking spectacles, and they have been among the most difficult to explain. Zoologists, studying bird and fish behavior with the help of miles of high-speed film, have often assumed some high level of coordination.

But now, gaining insight from new computer models, they see synchronized maneuvers as a surprising product of the actions of individual fish following individual rules for fleeing predators and staying clear of their neighbors. Thousands of simulated animals are programmed to fly or swim independently, and flock- and school-like behavior emerges on its own.

Despite recent progress, the science of analyzing the movements of flocks and schools is at an early stage in which scientists have identified many of these individual patterns but have yet to understand precisely how they emerge as movements of the group. Perhaps no conventional answer will ever emerge.

"The complexity is fascinating because there is so much going on, but it isn't unstructured—it isn't like dropping a thousand SuperBalls into a tank," said Craig W. Reynolds of Symbolics Corporation, who has modeled flocking and schooling. "The synchronization speed is pretty astounding. And since

birds aren't mental giants, they can't be doing deep thinking as they fly along. They must use fairly simple rules."

Flocks and schools are more than just groups of animals clumped together, and not all species display flocking and schooling behavior. Those that do, often in response to hungry predators, are capable of high-speed motion, flight around obstacles and abrupt course changes.

Herding can be a similar phenomenon, but land-bound animals cannot match the flexibility of birds and fish liberated in the three-dimensional space of air and water. The seemingly effortless rapport of thousands of animals has driven otherwise sober scientists to talk of "thought transference" and "magnetic field perturbation."

"All kinds of crazy things have been proposed," said Frank Heppner, a University of Rhode Island zoologist. "I once put forward my own bit of insanity by proposing that there had to be some biological radio."

Ornithologists have also traditionally believed that birds must be responding to cues from a leader—"because how else could you account for the near-simultaneous movement," Dr. Heppner said. Now, however, he and other zoologists believe that the motion can be explained along the lines of computer models in which no individual is a leader, or, in another sense, every individual is.

"Until very, very recently, there's been no conceptual model that permitted this," he said. "You have a situation where you have some simple rules, but growing out of those simple rules, you have emergent properties that have nothing to do with the original rules."

Behavior of Human Crowds

Wingless and finless creatures are also capable of coordinated motion with no leaders, as Dr. Heppner demonstrates with groups of hundreds of students. Asked to begin applauding en masse but in synchronization, they start with a random scattering of claps, yet manage to find a coordinated tempo almost instantly, usually within two beats.

Another kind of human behavior, the "wave" that rolls through masses of fans rising and sitting at a baseball stadium, may resemble the dynamics of a turning flock of birds. One zoologist, Wayne K. Potts, filmed the maneuvers of thousands of dunlin in Puget Sound, Washington, in 1983 and found that a turn propagates from one side of a flock to the other like a wave through a fluid.

The wave is fast. In the dunlin flocks, the turn spreads from bird to bird in about a 70th of a second—three times faster than a bird's reaction time. If a bird waited until its neighbors turned, it would be much too late.

Dr. Potts saw this as a perplexing challenge, in part because he had experience flying military aircraft in formation. Even simple formations, he felt, had a strong tendency to break up because of a time lag that tends to be magnified from pilot to pilot.

"If the first does something abrupt, the second is already behind," he said. "If anything like that was going on in a flock on a thousand birds, it would just be total chaos immediately. It's still underappreciated how difficult a problem it is."

"Chorus-Line Hypothesis"

Dr. Potts decided that birds must sense the approach of the wave from a distance and time their reactions accordingly. To test this idea—the "chorus-line hypothesis"—he provoked sudden maneuvers by shooting arrows near the edge of a flock. As expected, a turn began slowly with one or two birds and then accelerated rapidly through the rest.

Flocks and schools both execute far more complex maneuvers in the presence of a predator, and that is thought to be their evolutionary reason for being. Fish swimming in a more or less random way can instantly polarize—forming a dense school, aligned in parallel formation. And when a predator attacks, they can perform a fast expansion called the "fountain," quickly splaying outward from the intruder.

Traditionally, though their problems seem increasingly similar, flock experts and school experts have not worked together. Predators act differently in water and air, and the problems of how individual creatures perceive one another tend to be quite different.

Where birds rely on vision, for example, fish have another sense organ, known as the lateral line—"a sense of distant touch," as Julia Parrish of the University of California at Los Angeles put it. The lateral line allows them to respond sensitively to changes in water pressure caused by nearby motion.

The Problem with Starlings

Experimentally, those studying schools have had an advantage. Fish can be observed in laboratory tanks. "Whereas we're kind of stuck with a field situation,"

said Dr. Heppner, "because nobody has figured out how to get 10,000 starlings in a big cage and get them to do anything."

Even school experts, though, face daunting levels of ignorance. Researchers need to find out how much switching and shifting places of individuals takes place in a smoothly swimming school, for example. They wonder how different types and sizes of fish sort themselves out within a school.

Technologically, such questions pose a challenge. Watching the overall shape of a school or flock is one thing; picking out the paths of individual members is quite another, only now coming within reach of computer tracking systems.

"I think there's going to be a renaissance in studies of these groups," said William M. Hamner, a zoologist at the University of California at Los Angeles. "One needs to model them from a series of individual behaviors. One wants to take those individual behaviors and construct a whole from them."

Neither zoologists nor computer modelers know exactly what rules guide the motions of individual animals. In their models, they experiment with different possibilities. They do know that birds and fish must try to keep some minimal distance away from their neighbors, and they know that stragglers on the outskirts of a flock put themselves at risk if they stray.

Analyzing Films of Birds

Dr. Potts found from analyzing his films of dunlin that a left turn, say, starts not with the birds on the left side leading away, but rather with one or more birds turning inward from the right flank. That makes sense, he said, for individual birds fearing falcons and other raptors.

"The times when a bird is most vulnerable is when he's away," Dr. Potts said, "so the last thing he wants to do is turn outward."

Dr. Reynolds used a computer model to mimic such maneuvers. Instead of directing the motion of the whole flock, he allowed each bird to fly at certain speeds, moving on the basis of information about a limited number of neighbors.

"You get this fluid-seeming motion," he said. "The flock becomes a big amorphous thing that changes shape like a jellyfish, but there isn't a central mind, there isn't a flock mind."

Patterns Are Deceptive

The human tendency to see the whole as a coherent, willful entity has been misleading, Dr. Hamner said. The coordinated motion of a school or flock does not imply purposeful coordination on the part of individuals, and the feeling of purpose may be deceptive.

Looking down at freeway traffic from atop a skyscraper, Dr. Hamner said, with cars smoothly weaving in and out, one has to fight the illusion that all the cars are cooperating. On a more intimate scale, traffic does not seem quite so well planned.

"Flocks form patterns and the patterns entrain our brain," Dr. Hamner said. "We like patterns—we like patterns in waves, and we like patterns in a fire, and we see a flock of birds in the sky and we see a pattern in the overall movement. That's the beauty of the whole system, but it's also the thing that screws up human investigators."

November 24, 1987

Indestructible Wave May Hold Key to Superconductors

By JAMES GLEICK

Scientists struggling with the year's foremost problem in theoretical physics—how to explain the new high-temperature superconductivity—are focusing more and more on a peculiarly indestructible kind of wave known as a soliton.

Unlike ordinary waves, which tend to spread out and fade as they travel through a substance, solitons are coherent packets or pulses that retain their shape over long distances. Some physicists now believe that such pulses may help explain the ability of the new materials to carry electricity with no loss to resistance.

Whether these theorists, who include an unusual assortment of Nobel laureates, will succeed in explaining superconductivity with solitons is far from clear. "It's a lot of foment, it's really exciting, but it's by no means resolved," said David Campbell, director of the Center for Nonlinear Studies at Los Alamos National Laboratories.

But in the meantime, the soliton—part wave, part lump, part wrinkle in the fabric of matter and energy—is becoming a pervasive concern of modern science. In recent years, scientists have begun to recognize solitons in nature, taking shapes that range from giant internal waves in the oceans to strange, rolling cloud formations. And solitons in laser light promise to sharpen long-distance communication over optical fibers.

A soliton can be a true, single wave—the name's origin is "solitary wave"—or it can take the shape of some other stable, coherent structure in a complex system. "We've gradually realized that these things are far more common than we expected," said David Pines of the University of Illinois. "Under suitable circumstances, they can be present in almost all systems we know."

A vortex whirling in a draining tub of water behaves like a soliton. The red spot of Jupiter, a permanent giant eddy that sits amid the turbulence of the planet, now appears to be a soliton on a vast scale.

In the new superconductors, some theorists believe that solitons replace the ordinary waves of electronic energy that create electric current. Such solitons are particles that interact in a special way, colliding and passing through one another without losing their integrity.

"It brings us into a new conceptual domain of what a particle is," said Robert Schrieffer of the University of California at Santa Barbara, who shared the Nobel

Prize for creating the 30-year-old theory of superconductivity now being superseded. "Usually you think of starting out with bare particles in a vacuum and putting them into a medium. The soliton is a wrinkle of the medium itself. It's self-focusing, and it just doesn't dissipate."

Close to Perpetual Motion

Physicists puzzling over superconductivity have been trying to grasp the workings of a highly organized motion of electrons, flowing with perfect efficiency through a crystalline arrangement of molecules. It is the closest thing in nature to perpetual motion: an electrical current in a loop of a superconducting material will flow forever.

Experiment has run far ahead of theory in recent months. Scientists have discovered a new class of superconductors without understanding them. A successful theory will be necessary, however, for researchers hoping to find still better superconducting materials and to put them to practical use. Several alternatives, similar but incompatible, are now being put forward by competing theorists, each convinced that he is heading toward a solution, including Dr. Schrieffer, Philip W. Anderson of Princeton University and T. D. Lee of Columbia University.

The old theory was a triumph of solid-state physics known as the BCS model, after its creators, John Bardeen, Leon Cooper and Dr. Schrieffer. They found a special kind of bonding that lets electrons travel in coordinated pairs, eluding the obstacles that ordinarily scatter them as they travel through a molecular lattice.

Except at extremely low temperatures, however, the energy of thermal vibrations tends to break up the pairs, leaving the electrons subject to ordinary electrical resistance. Theorists trying to explain the high-temperature superconductors have been looking for a new kind of bonding.

"One of the things which has been confusing people is that they've just been expecting to see the same old stuff," Dr. Anderson said. "You're used to BCS, you've been brought up on BCS; in many cases, it's the biggest stretch of your imagination that you've ever had to undergo."

Physicists work out the invisible details of electron flow indirectly, by gathering magnetic and electrical data and assembling them into calculations. They find that electrons themselves, as quantum mechanical objects, cannot be treated as points in space; their calculations only work when each electron is treated as a bundle of probabilities distributed over some distance.

An especially odd quality of the electron pairs is that their members, though coordinated, remain relatively far apart in space. On average, between any two paired electrons, there are as many as a million others.

Marvin Cohen, a theorist at the University of California at Berkeley, compares the motion of such electrons to dancers, each bound to a partner far off in a crowded ballroom. "From the outside, it looks completely chaotic, but in fact it's completely organized," he said. "If your partner bumps into a pole and bounces, then, even though you don't have a pole, you have to bounce in the opposite direction. So there's a stability to the whole system."

The soliton models offer a different kind of coordination, more closely localized in real space. The solitons, whatever their precise electronic form—"spin bags," in one model, "holons and spinons" in another—represent tight, particle-like clusters.

Nonlinear Systems

Understanding why solitons arise in nature has been a challenge not only for physics but also for mathematics. They are leading examples of the kind of orderly structures that can arise only in nonlinear systems, systems that cannot be expressed in terms of simple, proportional relationships and are therefore notoriously hard to unravel.

When the influences on a wave are linear, as they are for light traveling through a vacuum, for example, solitons cannot occur. The waves tend to spread out. When a wave travels through a substance that responds nonlinearly, however, feedback can occur that organizes the wave and keeps it coherent.

For mathematicians, treating such phenomena as sets of equations, solitons are a kind of miracle. Ordinarily, nonlinear equations are especially hard to solve; yet in the case of solitons, a solution inexplicably appears.

Mathematicians are far from understanding when and why the usual complexities of nonlinearity collapse into such neat solutions. Physicists, though, have begun applying the idea so broadly that Dr. Schrieffer now warns against seeing solitons everywhere. "Everyone likes the word because it puts a little holy water on their ideas," he said.

A leading example of putting solitons to practical engineering use is in the laser light that carries telephone signals across long-distance networks of optical fibers. Ordinarily, these fibers behave as a linear medium. Over distances of many miles, the pulses degrade.

The standard solution is to install repeaters at regular intervals to reshape the signal. Researchers at A.T.&T. Bell Laboratories have found recently that, by increasing the intensity of the pulses enough, they can make the system nonlinear and produce solitons that retain their shape far longer.

"The Logjam of Data"

Physicists are far from gaining such precise control over the mechanisms of superconductivity. They are trying to match competing theories to the vast quantities of experimental data now pouring in from laboratories around the world, "trying to get the logjam of data to break up," as Dr. Anderson put it.

Solitons have an essential topological character, like a knot or a twist in a ribbon that can move from place to place but cannot be eliminated without untying the ribbon. Ian Stewart, a mathematician at the University of Warwick in England offers the example of an air bubble sliding under wet wallpaper, its shape maintained by the tension between forces of the air's pressure and the paper's elasticity.

Those studying superconductivity have been encouraged to think in topological terms by the peculiar structure of the newly found materials. In ordinary metals, electrons move freely in three dimensions. Experimentalists have discovered that the new superconductors have a complex crystal structure that reduces the freedom of motion to two dimensions or to one, along sheets and chains of copper atoms. In several theories, this reduced dimensionality is crucial to the formation of coherent motion leading to superconductivity.

The test of such theories, in the end, will lie in the data from experiments. But until a good theory exists, the data will remain hard to sort out and interpret, a classic scientific bind.

Dr. Anderson, for example, said that his own theory had succeeded in predicting several otherwise puzzling new measurements. But he acknowledged that other data do not fit so well—data that he believes will turn out to be irrelevant or wrong.

"Any of us who's any good at all is going to discard some of those experiments right off the bat," he said. He is confident that the remaining data will confirm his proposal.

On the other hand, so is Dr. Schrieffer. "Mother Nature will tell us who's right," he said.

December 15, 1987

The Quest for True Randomness Finally Appears Successful

By JAMES GLEICK

One of the strangest quests of modern computer science seems to be reaching its goal: mathematicians believe they have found a process for making perfectly random strings of numbers.

Sequences of truly patternless, truly unpredictable digits have become a perversely valuable commodity, in demand for a wide variety of applications in science and industry. Randomness is a tool for insuring fairness in statistical studies or jury selection, for designing safe cryptographic schemes and for helping scientists simulate complex behavior.

Yet random numbers—as unbiased and disorganized as the result of millions of imaginary coin tosses—have long proved extremely hard to make, either with electronic computers or mechanical devices. Consumers of randomness have had to settle for numbers that fall short, always hiding some subtle pattern.

How to use randomness, how to create it and how to recognize the real thing have become challenging questions in the computer era, touching many distant areas of science and philosophy. The randomness business is riddled with pitfalls; creeping non-randomness has undercut the expectations of many consumers, from state lotteries and tournament bridge players to drug manufacturers and court systems.

Random number generators are sold for every kind of computer. Every generator now in use has some kind of flaw, though often the flaws can be hard to detect. Furthermore, in a way, the idea of using a predictable electronic machine to create true randomness is nonsense. No string of numbers is really random if it can be produced by a simple computer process. But in a more practical sense, a string is random if there is no way to distinguish it from a string of coin flips.

"It's almost a contradiction," said Harvey Friedman, a logician at Ohio State University. "Superficially it's paradoxical, since you can just rerun the generator and get the same number."

Such paradoxes drew statisticians, computer scientists, probability theorists, physicists, philosophers and psychologists to an interdisciplinary conference on randomness organized by Dr. Friedman last week in Columbus.

"There's a whole philosophical kind of rethinking going on," Dr. Friedman said. "There are serious defects in just about everybody's way of looking at this."

Several theorists presented details of the apparent breakthrough in random-number generation, a technique that has emerged from a fast-growing area known as computational complexity, devoted to understanding the difficulty of solving different kinds of problems. The technique will now be subjected to batteries of statistical tests, meant to see whether it performs as well as the theorists believe it will. If it passes, computer scientists say it will be easy to put into use, either with software or with specially designed computer chips.

"The idea is very powerful, and it's clear that it would have a lot of unusual applications," said Leonid Levin, a Boston University mathematician.

The way people perceive randomness in the world around them differs sharply from the way mathematicians understand it and test for it. Asked to write down a "random" sequence of 100 zeroes and ones, for example, almost everyone chooses a sequence that alternates far too regularly. Although it seems paradoxical, if the zeroes and ones are too evenly mixed, they are not random.

A real sequence of 100 coin flips is likely to contain several strings of five or six consecutive heads or tails. Psychologists find that they have little trouble distinguishing real sequences from sequences that people write down: the sequences created by people taking psychology tests rarely contain streaks longer than four.

The need for randomness in human institutions seems to begin at whatever age "eeny meeny miny moe" becomes a practical decision-making procedure: randomness is meant to insure fairness. Like "eeny meeny miny moe," most such procedures prove far from random. Even the most carefully designed mechanical randomness-makers, from casino roulette wheels to the airblown Ping-Pong balls used by state lotteries, break down under scrutiny.

One such failure, on a dramatic scale, struck the national draft lottery in 1969, its first year. Military officials wrote all the possible birthdays on 366 pieces of paper and put them into 366 capsules. Then they poured the January capsules into a box and mixed them. Then they added the February capsules and mixed again—and so on.

At a public ceremony, the capsules were drawn from the box by hand. Only later did statisticians establish that the procedure had been far from random; people born toward the end of the year had a far greater chance of being drafted than people born in the early months.

In general, the problem of mixing or stirring or shuffling things to insure randomness is more complicated than most experts assume.

"Eventually things do get well mixed," said Persi Diaconis, a Harvard University statistician who has tested many mechanical randomizers and developed considerable mathematical theory for such problems. "The problem is, eventually we're all dead."

How long to mix can be a serious practical problem. Manufacturers mixing pill contents or foods want to avoid overmixing, because any such process takes time and because substances can break down chemically under too much stirring.

Drawbacks of Shuffling

Shuffling cards is a comparable problem. Dr. Diaconis has explored many methods and found the mathematics to be far from trivial. Using the standard riffle shuffle, for example, about seven shuffles are needed to get a good mix.

Oddly, if a riffle shuffle is carried out perfectly—the deck divided in half, then put back together with alternate cards from each half—it does not mix the structure at all. The order changes, but the structure remains. After eight perfect shuffles, the deck comes back exactly to its starting order.

A good mathematical description of real shuffling has to build in some randomness. It assumes that the deck is divided only approximately in half and then put back together with cards falling randomly from the left or right. It finds that, while seven shuffles are enough, six are not.

So Dr. Diaconis contends that millions of card-players are habitually under-shuffling. "Humans are really a lazy species, and people don't shuffle cards seven times," he said. "They shuffle three or four." The consequences have been, by game-playing standards, dire. When computerized dealing replaced real dealing in contract bridge tournaments, for example, experts noticed a difference: hands with outlandish distributions of cards in different suits seemed more common, and players suspected computer trouble.

In fact, the intuitions of bridge players had been shaped by generations of improperly shuffled cards. Playing a hand of bridge and gathering up the tricks tends to organize the deck into packets of four cards, many of them all the same suit. When the deck is reassembled, insufficiently mixed, and dealt again, the packets are divided evenly among the players, and the result is a distribution of suits that proves too normal—too many hands of 4-3-3-3 or 4-4-3-2.

The computers that replaced human dealers use random-number generators, or, more precisely, pseudorandom-number generators. A number is pseudorandom if it is produced by a deterministic process, so that the same starting point will produce the same result.

Uses in Science

State lotteries, like the draft lottery two decades ago, have held out against electronic versions, mainly for psychological reasons. People prefer to trust a drawing that they can see. But for most other purposes, pseudorandom-number generators are essential.

Physical scientists use them when they need to simulate some behavior that is too complicated to calculate directly. Social scientists and medical researchers often use them to randomize surveys and drug trials, in hopes of eliminating biases. Such biases can show up in insidious ways—even the process of reaching into a box and pulling out laboratory mice can lead to a non-random assortment that will prejudice medical research.

“There’s a lot of need for pseudorandom numbers, and the point is can you do it well and can you do it fast,” said Silvio Micali, a Massachusetts Institute of Technology computer scientist.

Dr. Micali is one of a loose group of mathematicians—also including Andrew Yao, Manuel Blum, Lenore Blum, Shafi Goldwasser and Michael Shub—who have developed the powerful new approach to the random number problem. Their method begins with mathematical processes that are easy to compute, but hard to reverse, known as one-way functions.

A classic example, and the example used in a particularly promising new pseudorandom-number generator, is the multiplication of two large prime numbers. The multiplication is easy; reversing the process is very hard. Given a large product of two primes, no one knows a fast way of factoring the number and finding the primes.

The new technique involves taking some starting number, multiplying it by itself, dividing by the product of two primes, taking the remainder and using it to repeat the process over and over again. The mathematicians have proved that there is a peculiar connection between the randomness of the outcome and the difficulty of factoring large numbers. Specifically, they have proved that if factoring large numbers is truly hard—as most believe likely—the resulting

sequence will be indistinguishable from true randomness.

Conversely, if some structure or pattern could be found in the sequence, that pattern would be, in effect, the long-sought solution to the factoring problem.

"It's very intuitive that randomness is the extreme case of hardness of computation," Dr. Micali said. "It lies at the heart of many sciences and many philosophical views of the universe. This makes that precise."

An expert in exposing the flaws in pseudorandom-number generators, George Marsaglia of Florida State University, has begun to test the new technique, along with several others, including one put forward by Stephen Wolfram of the Center for Complex Systems Research.

Dr. Marsaglia judges sequences not just by uniformity—a good distribution of numbers in a sequence—but also by "independence." No number or string of numbers should change the probability of the number or numbers that follow, any more than flipping a coin and getting 10 straight tails changes the likelihood of getting heads on the 11th flip.

He believes there will be a ready market for any improved pseudorandom-number generator. Tables of random digits have long been available; Dr. Marsaglia is planning to adapt that idea by producing a computer-era equivalent. His dream is a compact disk holding nothing but numbers—random sequences by the billions.

April 19, 1988

Coin-Tossing Computers Found to Show Subtle Bias

By MALCOLM W. BROWNE

When scientists use computers to try to predict complex trends and events, they often apply a type of calculation that requires long series of random numbers. But instructing a computer to produce acceptably random strings of digits is proving maddeningly difficult.

In deciding which team kicks off a football game, the toss of a real coin is random enough to satisfy all concerned. But the cost of even a slightly non-random string of electronic coin tosses can be devastating to both practical problem-solving and pure theory, and a new investigation has revealed that non-random computer tosses are much more common than many scientists had assumed.

Mathematical "models" designed to predict stock prices, atmospheric warming, airplane skin friction, chemical reactions, epidemics, population growth, the outcome of battles, the locations of oil deposits and hundreds of other complex matters increasingly depend on a statistical technique called Monte Carlo Simulation, which in turn depends on reliable and inexhaustible sources of random numbers.

Monte Carlo Simulation, named for Monaco's famous gambling casino, can help to represent very complex interactions in physics, chemistry, engineering, economics and environmental dynamics mathematically. Mathematicians call such a representation a "model," and if a model is accurate enough, it produces the same responses to manipulations that the real thing would do. But Monte Carlo modeling contains a dangerous flaw: if the supposedly random numbers that must be pumped into a simulation actually form some subtle, non-random pattern, the entire simulation (and its predictions) may be wrong.

The danger was highlighted in a recent report from Dr. Alan M. Ferrenberg and Dr. D. P. Landau of the University of Georgia at Athens and Dr. Y. Joanna Wong of the I.B.M. Corporation's Supercomputing center at Kingston, N.Y. In a Dec. 7 article in the journal *Physical Review Letters*, the scientists showed that five of the most popular computer programs for generating streams of random numbers produced errors when they were used in a simple mathematical model of the behavior of atoms in a magnetic crystal.

The reason for the errors, the scientists found, was that the numbers produced by all five programs were not random at all, despite the fact that they passed several statistical tests for randomness. Beneath their apparent randomness, the sequences actually concealed correlations and patterns, revealed only when the subtle non-randomness skewed the known properties of the crystal model.

All five of these systems for producing random numbers have long been used by scientists and statisticians with generally satisfactory results, Dr. Ferrenberg said. Major flaws turned up only recently when Dr. Ferrenberg and his colleagues were testing an ultra-powerful network of computers operating in parallel. Unlike ordinary sequential computer operations that execute programs one step at a time, parallel computing systems break up tasks into separate parts, which can be attacked simultaneously, with enormous savings in time. Parallel computers are so much faster and more powerful than the conventional kind that subtle problems in the programs they are executing come to light relatively quickly.

"We knew what the results of this test should be, and when we got errors for each simulation we tried, I thought there was something wrong with my program," Dr. Ferrenberg said. "But Dr. Wong suggested that the problem was with the random-number generators we were using, and she was right—a reminder that no known random-number system is foolproof for all applications."

Many relationships and interactions in science and engineering can be described by relatively simple mathematical equations that have definite solutions. But other systems are so complex that the equations describing their behavior, often containing many variables, cannot be solved by ordinary mathematical manipulations.

Disorder Hides Order

During the 1940s, Dr. Stanislaw M. Ulam, a mathematician recruited by Los Alamos National Laboratory to work on the atomic and hydrogen bombs, faced problems in the physics of nuclear explosions that proved too complicated to solve by conventional means. He attacked the problem by inventing Monte Carlo Simulation, in which, by filling in the blanks in his equations with successions of random numbers, he obtained probabilistic approximations of the answers the project needed.

This statistical system created an immediate demand for random numbers used in Monte Carlo equations, and the Rand Corporation of Santa Monica,

Calif., published an entire book containing nothing but random numbers. But in today's complex simulations, a program typically devours as many as 100 million random digits (binary zeros and ones) per second, Dr. Ferrenberg said, and to satisfy this prodigious appetite, a separate computer program must spit out digits at lightning speed. The need for speed means that any useful random number generator must contain only a few steps and be easy for a computer to execute.

Dr. Ron Graham, a mathematician at A.T. & T. Bell Laboratories in Murray Hill, N.J., explained that typical random-number generators may add a long series of arbitrary digits together, divide the result by some large number, and use the remainder as the basis for computing the next digit in the sequence.

But neither this nor any other machine-based system can produce truly random numbers. If computer-generated number sequences are long enough, repeating patterns inevitably emerge, even though they may remain hidden from their human creators.

Such patterns are sometimes discovered by accident. One system was believed to produce very good "pseudorandom" numbers, until someone plotted the numbers it produced on a three-dimensional graph. When that was done, the numbers proved to lie on a small number of planes rather than being uniformly distributed; in other words, the sequences were anything but random.

Dr. James Reeds, a computer expert at Bell, said the flaws exposed by Dr. Ferrenberg had caused problems for many users of Monte Carlo Simulations, including himself. "We all must take to heart the advice by the great John von Neumann, who wrote in 1951 that anyone who believed a computer could produce truly random sequences of numbers was living in a state of sin."

Catch-22 of Randomness

Random numbers are used not only by scientists but in primitive ciphers. Modern cryptographic systems, however, encipher secret messages between government officials and banks using techniques that do not depend on random numbers alone. Most modern high-level cipher systems are based on the products of two very large prime numbers, products that are enormously difficult to factor into the original primes.

Advanced cryptographic systems, besides hiding the content of secret messages, can produce sequences of random numbers that meet tests for randomness much more successfully than sequences from ordinary random number

generators. But they are far too slow for use in ordinary mathematical modeling.

There have been other ideas for improving the randomness of number sequences. Theorists have proposed that true random numbers rather than pseudorandom ones could be produced by machines responding to the radioactive decay of atoms. The instant at which a radioactive atom breaks up is completely unpredictable, even in theory, because it obeys the statistical rules of quantum mechanics, rather than any kind of causal determinism.

But Dr. Persi Diaconis, a Harvard University mathematician famous for his deep analyses of card shuffling and other approaches to randomness, believes that even atomic decay could pose problems. "Suppose such a decay were used to actuate a rotary switch, which would pick a number for the sequence," he said. "The mechanical switch could have some tiny imperfection that would bias the numbers in some way, so you would back where you started."

Another problem that would arise with any system producing genuinely random numbers, Dr. Diaconis said, is that no truly random sequence could be reproduced by the process that created it. In many cases, scientists need to be able to reproduce exact random sequences used in simulations, so that their work can be checked by others.

"We face a basic dilemma," Dr. Ferrenberg said. "We can no longer trust various random number systems that we used to think were pretty good. Now we must test every pseudorandom number generator we use, to see if it works for the particular application we have in mind. But to test it, we must know what the right answer should be, and that's what we're trying to find in the first place.

"I'm getting a lot of gray hair."

January 12, 1993

Science Squints at a Future Fogged by Chaotic Uncertainty

By MALCOLM W. BROWNE

Back during China's Shang dynasty, around 3,500 years ago, sages foretold the future by casting oracle bones—the clairvoyant equivalent of crap shooting.

Things have changed somewhat since then, even though predictions are as much in demand as ever, and even though we still send plenty of business to astrologers, tarot-card readers, numerologists, phrenologists, necromancers and psychics of all stripes. Aside from the traditional soothsayers, we sometimes also heed forecasts based on observations, scientific synthesis and reasoning.

Scientific sages depend not on tea leaves or the positions of planets but on tools like mathematical modeling, statistical analysis, complexity theory, celestial mechanics, geology, economics and epidemiology. Needless to say, scientists discount the naive paradigms of fortune tellers, ancient and modern.

Alas, rational approaches to prediction also fail all too often, and it may be that there are some phenomena for which predictions will remain forever out of reach.

As the stock market lurches between the tugs of bulls and bears, financial analysts armed with statistics and the latest marketing theories throw up their hands in despair when asked to guess what will happen from one day to the next.

Picnic planners know better than to rely on short-term weather forecasts, and meteorologists offer little hope that truly accurate weather predictions for specific places and times will ever be possible.

Relief agencies get little useful help from experts as they try to brace for disasters that might, with equal likelihood, occur tomorrow or a thousand years from now. Understanding the mechanisms of events like earthquakes and volcanoes offers little help in predicting precisely when they will occur.

Geologists have a pretty good idea that earthquakes are caused by the movement of tectonic plates, yet the art of earthquake forecasting remains notoriously imprecise.

The largest earthquake in four years—an 8.2-magnitude tremor centered under the ocean between Australia and Antarctica—caught seismologists completely off guard when it shook the sea floor last March 25, and geologists are still puzzled by the quake; it did not occur at the junction of tectonic plates where most quakes occur, but struck within a single plate.

Future seismic surprises, including those causing catastrophic loss of life, seem inevitable.

The tsunami that roared over Papua New Guinea on July 17, killing more than 2,000 people, caught everyone by surprise. Experts excused their failure to warn the population on the ground that a giant tsunami wave materializes only when a scarcely noticeable wave spawned by an earthquake or some other event far out at sea reaches shallow coastal water. By then it is almost on top of some hapless coastline, leaving no time to prepare.

There have been recent reminders that even in principle, some things are impossible to predict.

Among the puzzles that have perplexed mathematicians and physicists at least since the time of Isaac Newton in the 17th century is the "N-body problem" (sometimes called the "Many-body problem").

One of Newton's monumental discoveries was that any two objects attract each other with a force proportional to their masses and inversely proportional to the square of their distance apart. But when three or more objects—the sun, the earth and the moon, for example—are interacting gravitationally, exact solutions of the equations describing their motions generally remain beyond reach.

Fortunately, since Newton's day, some very good approximate solutions of N-body equations have been devised, and such solutions have allowed space scientists to send vehicles to the distant reaches of the solar system with astounding precision.

This month, Dr. Gregory R. Buck of Saint Anselm College, in Manchester, N.H., disclosed a new class of approximate N-body solutions based on the analogy of a closed loop of beads, in which the beads, evenly spaced, chase each other around the curves and tangles of the loop. The system may help to work out the interactions of particles within a plasma, Dr. Buck suggested.

But none of the approximations now known exactly solve Newton's equations, and this means that the motions of asteroids and comets can be predicted only up to a certain point in the distant future. Beyond that, forecasting an impact by one of these objects on the earth may be intrinsically impossible. A hit or miss

may depend so sensitively on the minuscule "initial conditions" of all the objects involved that precise calculation becomes impossible. This is a property of a large class of systems scientists describe as chaotic.

Long-term foreknowledge of the hit or miss—a question of life or death for millions—is ruled out by the chaos inherent in the N-body system.

Scientists have yet to come to terms with chaos in all its manifestations. Dr. Steven Weinberg, winner of a Nobel Prize in physics, once said he considered an understanding of chaotic turbulence in fluids as the single most intractable problem in physics. Until scientists reach a deeper understanding of turbulence, many physicists believe, the dynamics of climate change, the behavior of galaxies and many other phenomena can never be fully penetrated.

Chaos can also prevent reliable predictions of group decisions, including those that investors make. Group decisions by investors can cause chaotic price fluctuations of commodities that are intrinsically unpredictable, it seems.

In a report published Aug. 24 in the journal *Physical Review Letters*, Dr. David A. Meyer of the University of California at San Diego and Dr. Thad A. Brown of the University of Missouri presented formal proof that collective decisions can be chaotic, even when the views of all participants are known and a standard voting rule is strictly applied.

When a group of decision-makers must choose between three or more options by comparing two of them at a time, the collective outcome often depends on the order in which the choices are presented. The outcome can cycle chaotically, the mathematicians found. Even nonhuman decision-makers—the computers that buy and sell commodities according to programmed rules, for example—are subject to chaotic uncertainty, a situation in which prediction becomes impossible.

Frustrated by the complex and chaotic behavior of the real world, some theorists have invented forecasting techniques based on little more than pure mathematics.

In the 1970s, René Thom, a French mathematician, developed an approach called Catastrophe Theory, which, for a time, enjoyed a considerable vogue among physicists, biologists and even sociologists. The theory is an application of topology, a field of mathematics that deals with the shapes of surfaces.

Dr. Thom's theory holds that many sequences of events can be represented as smooth trajectories along a saddle-shaped surface, at one point of which an abrupt discontinuity, or "catastrophe cusp," shunts them off to one side of the saddle or the other.

Dr. Thom and his followers proposed that mathematical models based on catastrophe cusps could be used to predict the reproduction of bacteria, the behavior of the stock market, heart attacks, biological evolution and the outbreak of war, among many other things. To some, Dr. Thom's theory seemed to offer an explanation of almost everything, but many others condemned it as useless. Today, Catastrophe Theory is all but forgotten.

Predicting life spans in the absence of detailed knowledge has long interested scientists as well as insurance statisticians. A forecast of life expectancy based on the average age at death of a person's four grandparents is a simple example of statistical forecasting. But a much more daring approach was devised a few years ago by Dr. J. Richard Gott 3d, a professor of astrophysics at Princeton University.

Dr. Gott's scheme is based on the "Copernican principle," which assumes that the odds are overwhelmingly against any particular place or time being "special." From this, Dr. Gott reasoned that the mere knowledge of how long something (or someone) has been around is sufficient to estimate how much longer it could last. Based on this system, and the assumption that *Homo sapiens* appeared on earth about 200,000 years ago, Dr. Gott calculated that intelligent human beings are 95 percent certain to survive a minimum of 5,128 years more, and a maximum of 7.8 million years more.

There are those who contend that predictions like these are so vague that they are scarcely more useful than the prophecies of the Delphic oracle in ancient Greece, which was consulted by Socrates, Oedipus and other luminaries of the day. The oracle (operated by a concealed priest or priestess) was so ambiguous it could nearly never be proved wrong.

Scientists will never be able to answer all our questions about future events or to satisfy a deep-seated human yearning to foresee what's coming at us. Some scientific efforts at prediction will always be defeated by the nature of Nature.

Mystic oracles have never shed light on future events either, but even 1,398 years after Socrates's suicide, legions of people continue to visit palmists, astrologists and psychics. It's human to prefer something to nothing at all.

September 22, 1998

Probing Disease Clusters: Easier to Spot Than Prove

By GINA KOLATA

The trouble began when Bobbie Gallagher noticed that her two-year-old daughter was behaving strangely, obsessively spinning and scrupulously setting her toys in rows. Alanna Gallagher turned out to have autism, a rare neurological disorder of unknown cause.

So did Alanna's little brother. So did about 40 other children who lived in the Gallaghers' town of Brick, N.J., near the seashore.

The parents in Brick were alarmed. On average, 1 child in 500 is autistic; in the town, the figure is about three times that.

But what does it mean? Does Brick have toxic chemicals in the water, pollutants in the air?

The problem, scientists say, may be impossible to resolve. It was yet another instance of a phenomenon that makes many statisticians shudder. It was a disease cluster—the Boy Who Cried Wolf of epidemiology.

Every time a disease cluster turns up, communities worry, scientists scramble for a cause and, as in the new movie based on Jonathan Harr's 1995 book, *A Civil Action* (Random House), about a leukemia cluster in Woburn, Mass., lawyers start suing. Yet over and over again, despite years—sometimes decades—of efforts to link the disease with a cause, scientists usually come up empty-handed.

It can sound paradoxical. Here are unusual numbers of people with a disease. Toxic chemicals are everywhere, and many of them cause cancers and other diseases in laboratory animals. Why should it be so hard to find a cause?

Some disease clusters have been successfully linked to toxins: Coal miners got black lung disease; asbestos workers got mesothelioma. Workers cleaning containers where polyvinyl chloride was synthesized, breathing in fumes, got cancer of the blood vessels of the liver until machines replaced them.

But these examples of proven cause and effect are the rare exceptions, statisticians say. And they have two things in common: The chemical exposure was enormous, and the disease was extraordinarily rare.

Most disease clusters are very different. Autism, breast cancer and leukemia are fairly common. And even when there does seem to be an unusually high incidence of a disease, the search for a chemical basis usually turns up minute

amounts of toxic substances that also are found in other places where there are no clusters. In other words, linking the suspect chemicals to the disease can be very hard. It can also be difficult to know if a cluster is anything more than a chance occurrence. And chance is hard to ignore.

Clusters will naturally appear even when events occur at random, said Dr. Persi Diaconis, a statistician at Stanford University. "There was a famous example of this when bombs were hitting London during World War II," he said. "People were sure they were targeting individual places and they made up the most elaborate scenarios" to explain how the bomb targets were selected. But in the end, when the pattern was analyzed, the bombing turned out to be random.

Another problem is how to draw the boundaries of a cluster.

Dr. James Robins, a statistician at Harvard University's School of Public Health, said it is a natural tendency to draw boundaries around groups of events to make clusters happen. If there are three children with cancer on a single block, you may draw your circle around the block—making that a cluster—rather than around the town as a whole, which may show no cluster.

Say you do find a cluster. Unless you identify, say, black lung or mesothelioma, statisticians say, the next question is: How can you decide if the cluster was caused by blind random clumpings of cases, with no environmental cause, or by a toxin in the environment?

Why would only one town have a disease cluster, some experts ask, while other places with the same pollutants in the air or water do not? One possibility might be an unidentified chemical in a mix of pollutants that is unique to the town. But that, of course, raises questions of how to find it.

Finally, there is the indirect exposure problem. If there is no direct link between chemicals and a disease, the tendency is to look for other exposures. Could the fathers, for example, have had their sperm affected when they were growing up? Or could the mothers have been exposed to chemicals during pregnancy? Some statisticians say that if people look hard enough and slice the data enough ways an association will emerge. What it means is another question.

Others are optimistic. Suzanne Condon, the director of the bureau of environmental health assessment at the Massachusetts Department of Public Health, said that in an unpublished study her department found that in the Woburn case, women who drank water from certain wells when they were pregnant were more likely to have children who developed leukemia. "We believe this sheds a lot of light on what happened in Woburn," she said. W. R. Grace, which was accused

along with Beatrice Foods of dumping chemicals in a way that allowed them to reach the water supply, paid \$8 million into a settlement fund. Both companies agreed to finance an expensive cleanup plan.

The Massachusetts health department, however, warned on its Web page, "Findings should be interpreted with caution due to the limitations of conducting statistical analyses on small populations."

That may not be what people want to hear, statisticians concede. "People—and I, too—find it hard to accept that it is just random chance that brought this horrible consequence," said Dr. David Freedman, a statistician at the University of California at Berkeley.

Some statisticians ask whether it is worthwhile to keep pouring money and effort into searches for clusters and searches to explain them.

"The question is, at what point do you say we've see too many like this?" Dr. Robins asked. "Huge amounts of money" have gone to study disease clusters where the suspected cause was tiny amounts of chemicals, he added, and so far, "nothing has come of it."

January 31, 1999

The Odds of That

By LISA BELKIN

When the Miami police first found Benito Que, he was slumped on a desolate side street, near the empty spot where he had habitually parked his Ford Explorer. At about the same time, Don C. Wiley mysteriously disappeared. His car, a white rented Mitsubishi Galant, was abandoned on a bridge outside of Memphis, where he had just had a jovial dinner with friends. The following week, Vladimir Pasechnik collapsed in London, apparently of a stroke.

The list would grow to nearly a dozen in the space of four nerve-jangling months. Stabbed in Leesburg, Va. Suffocated in an air-locked lab in Geelong, Australia. Found wedged under a chair, naked from the waist down, in a blood-splattered apartment in Norwich, England. Hit by a car while jogging. Killed in a private plane crash. Shot dead while a pizza delivery man served as a decoy.

What joined these men was their proximity to the world of bioterror and germ warfare. Que, the one who was car-jacked, was a researcher at the University of Miami School of Medicine. Wiley, the most famous, knew as much as anyone about how the immune system responds to attacks from viruses like Ebola. Pasechnik was Russian, and before he defected, he helped the Soviets transform cruise missiles into biological weapons. The chain of deaths—these three men and eight others like them—began last fall, back when emergency teams in moonsuits were scouring the Capitol, when postal workers were dying, when news agencies were on high alert and the entire nation was afraid to open its mail.

In more ordinary times, this cluster of deaths might not have been noticed, but these are not ordinary times. Neighbors report neighbors to the F.B.I.; passengers are escorted off planes because they make other passengers nervous; medical journals debate what to publish, for fear the articles will be read by evil eyes. Now we are spooked and startled by stories like these—all these scientists dying within months of one another, at the precise moment when tiny organisms loom as a gargantuan threat. The stories of these dozen or so deaths started out as a curiosity and were transformed rumor by rumor into the specter of conspiracy as they circulated first on the Internet and then in the mainstream media. What are the odds, after all?

What are the odds, indeed?

For this is not about conspiracy but about coincidence—unexpected connections that are both riveting and rattling. Much religious faith is based on the idea that almost nothing is coincidence; science is an exercise in eliminating the taint of coincidence; police work is often a feint and parry between those trying to prove coincidence and those trying to prove complicity. Without coincidence, there would be few movies worth watching (“Of all the gin joints in all the towns in all the world, she walks into mine”), and literary plots would come grinding to a disappointing halt. (What if Oedipus had not happened to marry his mother? If Javert had not happened to arrive in the town where Valjean was mayor?)

The true meaning of the word is “a surprising concurrence of events, perceived as meaningfully related, with no apparent causal connection.” In other words, pure happenstance. Yet by merely noticing a coincidence, we elevate it to something that transcends its definition as pure chance. We are discomforted by the idea of a random universe. Like Mel Gibson’s character Graham Hess in M. Night Shyamalan’s new movie *Signs*, we want to feel that our lives are governed by a grand plan.

The need is especially strong in an age when paranoia runs rampant. “Coincidence feels like a loss of control perhaps,” says John Allen Paulos, a professor of mathematics at Temple University and the author of *Innumeracy*, the improbable best-seller about how Americans don’t understand numbers. Finding a reason or a pattern where none actually exists “makes it less frightening,” he says, because events get placed in the realm of the logical. “Believing in fate, or even conspiracy, can sometimes be more comforting than facing the fact that sometimes things just happen.”

In the past year there has been plenty of conspiracy, of course, but also a lot of things have “just happened.” And while our leaders are out there warning us to be vigilant, the statisticians are out there warning that patterns are not always what they seem. We need to be reminded, Paulos and others say, that most of the time patterns that seem stunning to us aren’t even there. For instance, although the numbers 9/11 (9 plus 1 plus 1) equal 11, and American Airlines Flight 11 was the first to hit the twin towers, and there were 92 people on board (9 plus 2), and Sept. 11 is the 254th day of the year (2 plus 5 plus 4), and there are 11 letters each in “Afghanistan,” “New York City” and “the Pentagon” (and while we’re counting, in George W. Bush), and the World Trade towers themselves took the form of the number 11, this seeming numerical message is not actually a pattern that exists but merely a pattern we have found. (After all, the second flight to hit the towers

was United Airlines Flight 175, and the one that hit the Pentagon was American Airlines Flight 77, and the one that crashed in a Pennsylvania field was United Flight 93, and the Pentagon is shaped, well, like a pentagon.)

The same goes for the way we think of miraculous intervention. We need to be told that those lucky last-minute stops for an Egg McMuffin at McDonald's or to pick up a watch at the repair shop or to vote in the mayoral primary—stops that saved lives of people who would otherwise have been in the towers when the first plane hit—certainly looked like miracles but could have been predicted by statistics. So, too, can the most breathtaking of happenings—like the sparrow that happened to appear at one memorial service just as a teenage boy, at the lectern eulogizing his mom, said the word “mother.” The tiny bird lighted on the boy's head; then he took it in his hand and set it free.

Something like that has to be more than coincidence, we protest. What are the odds? The mathematician will answer that even in the most unbelievable situations, the odds are actually very good. The law of large numbers says that with a large enough denominator—in other words, in a big wide world—stuff will happen, even very weird stuff. “The really unusual day would be one where nothing unusual happens,” explains Persi Diaconis, a Stanford statistician who has spent his career collecting and studying examples of coincidence. Given that there are 280 million people in the United States, he says, “280 times a day, a one-in-a-million shot is going to occur.”

Throw your best story at him—the one about running into your childhood playmate on a street corner in Azerbaijan or marrying a woman who has a birthmark shaped like a shooting star that is a perfect match for your own or dreaming that your great-aunt Lucy would break her collarbone hours before she actually does—and he will nod politely and answer that such things happen all the time. In fact, he and his colleagues also warn me that although I pulled all examples in the prior sentence from thin air, I will probably get letters from readers saying one of those things actually happened to them.

And what of the deaths of nearly a dozen scientists? Is it really possible that they all just happened to die, most in such peculiar, jarring ways, within so short a time? “We can never say for a fact that something isn't a conspiracy,” says Bradley Efron, a professor of statistics at Stanford. “We can just point out the odds that it isn't.”

I first found myself wondering about coincidence last spring when I read a small news item out of the tiny Finnish town of Raahe, which is 370 miles north

of Helsinki. On the morning of March 5, two elderly twin brothers were riding their bicycles, as was their habit, completing their separate errands. At 9:30, one brother was struck by a truck along coastal Highway 8 and killed instantly. About two hours later and one mile down the same highway, the other brother was struck by a second truck and killed.

"It was hard to believe this could happen just by chance," says Marko Salo, the senior constable who investigated both deaths for the Raahe police department. Instead, the department looked for a cause, thinking initially that the second death was really a suicide.

"Almost all Raahe thought he did it knowing that his brother was dead," Salo says of the second brother's death. "They thought he tried on purpose. That would have explained things." But the investigation showed that the older brother was off cheerfully getting his hair cut just before his own death.

The family could not immediately accept that this was random coincidence, either. "It was their destiny," offers their nephew, who spoke with me on behalf of the family. It is his opinion that his uncles shared a psychic bond throughout their lives. When one brother became ill, the other one fell ill shortly thereafter. When one reached to scratch his nose, the other would often do the same. Several years ago, one brother was hit and injured by a car (also while biking), and the other one developed pain in the same leg.

The men's sister had still another theory entirely. "She worried that it was a plot to kill both of them," the nephew says, describing his aunt's concerns that terrorists might have made their way to Raahe. "She was angry. She wanted to blame someone. So she said the chances of this happening by accident are impossible."

Not true, the statisticians say. But before we can see the likelihood for what it is, we have to eliminate the distracting details. We are far too taken, Efron says, with superfluous facts and findings that have no bearing on the statistics of coincidence. After our initial surprise, Efron says that the real yardstick for measuring probability is "How surprised should we be?" How surprising is it, to use this example, that two 70-year-old men in the same town should die within two hours of each other? Certainly not common, but not unimaginable. But the fact that they were brothers would seem to make the odds more astronomical. This, however, is a superfluous fact. What is significant in their case is that two older men were riding bicycles along a busy highway in a snowstorm, which greatly increases the probability that they would be hit by trucks.

Statisticians like Efron emphasize that when something striking happens, it only incidentally happens to us. When the numbers are large enough, and the distracting details are removed, the chance of anything is fairly high. Imagine a meadow, he says, and then imagine placing your finger on a blade of grass. The chance of choosing exactly that blade of grass would be one in a million or even higher, but because it is a certainty that you will choose a blade of grass, the odds of one particular one being chosen are no more or less than the one to either side.

Robert J. Tibshirani, a statistician at Stanford University who proved that it was probably not coincidence that accident rates increase when people simultaneously drive and talk on a cellphone, leading some states to ban the practice, uses the example of a hand of poker. "The chance of getting a royal flush is very low," he says, "and if you were to get a royal flush, you would be surprised. But the chance of any hand in poker is low. You just don't notice when you get all the others; you notice when you get the royal flush."

When these professors talk, they do so slowly, aware that what they are saying is deeply counterintuitive. No sooner have they finished explaining that the world is huge and that any number of unlikely things are likely to happen than they shift gears and explain that the world is also quite small, which explains an entire other type of coincidence. One relatively simple example of this is "the birthday problem." There are as many as 366 days in a year (accounting for leap years), and so you would have to assemble 367 people in a room to absolutely guarantee that two of them have the same birthday. But how many people would you need in that room to guarantee a 50 percent chance of at least one birthday match?

Intuitively, you assume that the answer should be a relatively large number. And in fact, most people's first guess is 183, half of 366. But the actual answer is 23. In Paulos's book, he explains the math this way: "[T]he number of ways in which five dates can be chosen (allowing for repetitions) is $(365 \times 365 \times 365 \times 365 \times 365)$. Of all these 365^5 ways, however, only $(365 \times 364 \times 363 \times 362 \times 361)$ are such that no two of the dates are the same; any of the 365 days can be chosen first, any of the remaining 364 can be chosen second and so on. Thus, by dividing this latter product $(365 \times 364 \times 363 \times 362 \times 361)$ by 365^5 , we get the probability that five persons chosen at random will have no birthday in common. Now, if we subtract this probability from 1 (or from 100 percent if we're dealing with percentages), we get the complementary probability that at least two of the five people do have a birthday in common. A similar calculation

using 23 rather than 5 yields $\frac{1}{2}$, or 50 percent, as the probability that at least 2 of 23 people will have a common birthday."

Got that?

Using similar math, you can calculate that if you want even odds of finding two people born within one day of each other, you only need 14 people, and if you are looking for birthdays a week apart, the magic number is seven. (Incidentally, if you are looking for an even chance that someone in the room will have your exact birthday, you will need 253 people.) And yet despite numbers like these, we are constantly surprised when we meet a stranger with whom we share a birth date or a hometown or a middle name. We are amazed by the overlap—and we conveniently ignore the countless things we do not have in common.

Which brings us to the death of Benito Que, who was not, despite reports to the contrary, actually a microbiologist. He was a researcher in a lab at the University of Miami Sylvester Cancer Center, where he was testing various agents as potential cancer drugs. He never worked with anthrax or any infectious disease, according to Dr. Bach Ardalan, a professor of medicine at the University of Miami and Que's boss for the past three years. "There is no truth to the talk that Benito was doing anything related to microbiology," Ardalan says. "He certainly wasn't doing any sensitive kind of work that anyone would want to hurt him for."

But those facts got lost amid the confusion—and the prevalence of very distracting details—in the days after he died. So did the fact that he had hypertension. On the afternoon of Monday, Nov. 19, Que attended a late-afternoon lab meeting, and as it ended, he mentioned that he hadn't been feeling well. A nurse took Que's blood pressure, which was 190/110. "I wanted to admit him" to the hospital, Ardalan says, but Que insisted on going home.

Que had the habit of parking his car on Northwest 10th Avenue, a side street that Ardalan describes as being "beyond the area considered to be safe." His spot that day was in front of a house where a young boy was playing outside. Four youths approached Que as he neared his car, the boy later told the police, and there might have been some baseball bats involved. When the police arrived, they found Que unconscious. His briefcase was at his side, but his wallet was gone. His car was eventually found abandoned several miles from the scene. He was taken to the hospital, the same one at which he worked, where he spent more than a week in a coma before dying without ever regaining consciousness.

The mystery, limited to small items in local Florida papers at first, was, What killed Benito Que? Could it have been the mugging? A CAT scan showed no signs

of bone fracture. In fact, there were no scrapes or bruises or other physical signs of assault. Perhaps he died of a stroke? His brain scan did show a "huge intracranial bleed," Ardalan says, which would have explained his earlier headache, and his high blood pressure would have made a stroke likely.

In other words, this man just happened to be mugged when he was a stroke waiting to be triggered. That is a jarring coincidence, to be sure. But it is not one that the world was likely to have noticed if Don Wiley had not up and disappeared.

Don C. Wiley was a microbiologist. He did some work with anthrax, and a lot of work with H.I.V., and he was also quite familiar with Ebola, smallpox, herpes and influenza. At 57, he was the father of four children and a professor of biochemistry and biophysics in the department of molecular and cellular biology at Harvard.

On Nov. 15, four days before the attack on Benito Que, Wiley was in Memphis to visit his father and to attend the annual meeting of the scientific advisory board of St. Jude's Research Hospital, of which he was a member. At midnight, he was seen leaving a banquet at the Peabody Hotel in downtown Memphis. Friends and colleagues say he had a little to drink but did not appear impaired, and they remember him as being in a fine mood, looking forward to seeing his wife and children, who were about to join him for a short vacation.

Wiley's father lives in a Memphis suburb, and that is where Wiley should have been headed after the banquet. Instead, his car was found facing in the opposite direction on the Hernando DeSoto Bridge, which spans the Mississippi River at the border of Tennessee and Arkansas. When the police found the car at 4 a.m., it was unlocked, the keys were in the ignition and the gas tank was full. There was a scrape of yellow paint on the driver's side, which appeared to come from a construction sign on the bridge, and a right hubcap was missing on the passenger side, where the wheel rims were also scraped. There was no sign, however, of Don Wiley.

The police trawled the muddy Mississippi, but they didn't really expect to find him. Currents run fast at that part of the river, and a body would be quickly swept away. At the start of the search, they thought he might have committed suicide; others had jumped from the DeSoto Bridge over the years. Detectives searched Wiley's financial records, his family relationships, his scientific research—anything for a hint that the man might have had cause to take his own life.

Finding nothing, the investigation turned medical. Wiley, they learned, had a seizure disorder that he had hidden from all but family and close friends. He had

a history of two or three major episodes a year, his wife told investigators, and the condition was made worse when he was under stress or the influence of alcohol. Had Wiley, who could well have been tired, disoriented by bridge construction and under the influence of a few drinks, had a seizure that sent him over the side of the bridge?

That was the theory the police spoke of in public, but they were also considering something else. The week that Wiley disappeared coincided with the peak of anthrax fear throughout the country. Tainted letters appeared the month before at the Senate and the House of Representatives. Two weeks earlier, a New York City hospital worker died of inhaled anthrax. Memphis was not untouched by the scare; a federal judge and two area congressmen each received hoax letters. Could it be mere chance that this particular scientist, who had profound knowledge of these microbes, had disappeared at this time?

"The circumstances were peculiar," says George Bolds, a spokesman for the Memphis bureau of the F.B.I., which was called in to assist. "There were questions that had to be asked. Could he have been kidnapped because his scientific abilities would have made him capable of creating anthrax? Or maybe he'd had some involvement in the mailing of the anthrax, and he'd disappeared to cover his tracks? Did his co-conspirators grab him and kill him?"

"We were in new territory," Bolds continued. "Just because something is conceivable doesn't mean it's actually happened, but at the same time, just because it's never happened before doesn't mean it can't happen. People's ideas of what is possible definitely changed on Sept. 11. People feel less secure and less safe. I'm not sure that they're at greater risk than they were before. Maybe they're just more aware of the risk they are actually at."

As a species, we appear to be biologically programmed to see patterns and conspiracies, and this tendency increases when we sense that we're in danger. "We are hard-wired to overreact to coincidences," says Persi Diaconis. "It goes back to primitive man. You look in the bush, it looks like stripes, you'd better get out of there before you determine the odds that you're looking at a tiger. The cost of being flattened by the tiger is high. Right now, people are noticing any kind of odd behavior and being nervous about it."

Adds John Allen Paulos: "Human beings are pattern-seeking animals. It might just be part of our biology that conspires to make coincidences more meaningful than they really are. Look at the natural world of rocks and plants and rivers: it doesn't offer much evidence for superfluous coincidences, but primitive

man had to be alert to all anomalies and respond to them as if they were real."

For decades, all academic talk of coincidence has been in the context of the mathematical. New work by scientists like Joshua B. Tenenbaum, an assistant professor in the department of brain and cognitive sciences at M.I.T., is bringing coincidence into the realm of human cognition. Finding connections is not only the way we react to the extraordinary, Tenenbaum postulates, but also the way we make sense of our ordinary world. "Coincidences are a window into how we learn about things," he says. "They show us how minds derive richly textured knowledge from limited situations."

To put it another way, our reaction to coincidence shows how our brains fill in the factual blanks. In an optical illusion, he explains, our brain fills the gaps, and although people take it for granted that seeing is believing, optical illusions prove that's not true. "Illusions also prove that our brain is capable of imposing structure on the world," he says. "One of the things our brain is designed to do is infer the causal structure of the world from limited information."

If not for this ability, he says, a child could not learn to speak. A child sees a conspiracy, he says, in that others around him are obviously communicating and it is up to the child to decode the method. But these same mechanisms can misfire, he warns. They were well suited to a time of cavemen and tigers and can be overloaded in our highly complex world. "It's why we have the urge to work everything into one big grand scheme," he says. "We do like to weave things together."

"But have we evolved into fundamentally rational or fundamentally irrational creatures? That is one of the central questions."

We pride ourselves on being independent and original, and yet our reactions to nearly everything can be plotted along a predictable spectrum. When the grid is coincidences, one end of the scale is for those who believe that these are entertaining events with no meaning; at the other end are those who believe that coincidence is never an accident.

The view of coincidence as fate has lately become something of a minitrend in the New Age section of bookstores. Among the more popular authors is SQuire Rushnell (who, in the interest of marketing, spells his first name with a capital Q). Rushnell spent 20 years producing such television programs as *Good Morning America* and *Schoolhouse Rock*. His fascination with coincidence began when he learned that both John Adams and Thomas Jefferson died on the same July 4, 50 years after the ratification of the Declaration of Independence.

"That stuck in my craw," Rushnell says, "and I couldn't stop wondering what that means." And so Rushnell wrote *When God Winks: How the Power of Coincidence Guides Your Life*. The book was published by a small press shortly before Sept. 11 and sold well without much publicity. It will be rereleased with great fanfare by Simon & Schuster next month. Its message, Rushnell says, is that "coincidences are signposts along your universal pathway. They are hints that you are going in the right direction or that you should change course. It's like your grandmother sitting across the Thanksgiving table from you and giving you a wink. What does that wink mean? 'I'm here, I love you, stay the course.'"

During my interview with Rushnell, I told him the following story: On a frigid December night many years ago, a friend dragged me out of my warm apartment, where I planned to spend the evening in my bathrobe nursing a cold. I had to come with her to the movies, she said, because she had made plans with a pal from her office, and he was bringing a friend for me to meet. Translation: I was expected to show up for a last-minute blind date. For some reason, I agreed to go, knocking back a decongestant as I left home. We arrived at the theater to find that the friend who was supposed to be my "date" had canceled, but not to worry, another friend had been corralled as a replacement. The replacement and I both fell asleep in the movie (I was sedated by cold medicine; he was a medical resident who had been awake for 36 hours), but four months later we were engaged, and we have been married for nearly 15 years.

Rushnell was enthralled by this tale, particularly by the mystical force that seemed to have nudged me out the door when I really wanted to stay home and watch *The Golden Girls*. I know that those on the other end of the spectrum—the scientists and mathematicians—would have offered several overlapping explanations of why it was unremarkable.

There are, of course, the laws of big numbers and small numbers—the fact that the world is simultaneously so large that anything can happen and so small that weird things seem to happen all the time. Add to that the work of the late Amos Tversky, a giant in the field of coincidence theory, who once described his role in this world as "debugging human intuition." Among other things, Tversky disproved the "hot hand" theory of basketball, the belief that a player who has made his last few baskets will more likely than not make his next. After examining thousands of shots by the Philadelphia 76ers, he proved that the odds of a successful shot cannot be predicted by the shots that came before.

Tversky similarly proved that arthritis sufferers cannot actually predict the weather and are not in more pain when there's a storm brewing, a belief that began with the ancient Greeks. He followed 18 patients for 15 months, keeping detailed records of their reports of pain and joint swelling and matching them with constantly updated weather reports. There was no pattern, he concluded, though he also conceded that his data would not change many people's beliefs.

We believe in such things as hot hands and arthritic forecasting and predestined blind dates because we notice only the winning streaks, only the chance meetings that lead to romance, only the days that Grandma's hands ache before it rains. "We forget all the times that nothing happens," says Ruma Falk, a professor emeritus of psychology at Hebrew University in Jerusalem, who studied years ago with Tversky. "Dreams are another example," Falk says. "We dream a lot. Every night and every morning. But it sometimes happens that the next day something reminds you of that dream. Then you think it was a premonition."

Falk's work is focused on the question of why we are so entranced by coincidence in the first place. Her research itself began with a coincidence. She was on sabbatical in New York from her native Israel, and on the night before Rosh Hashana she happened to meet a friend from Jerusalem on a Manhattan street corner. She and the friend stood on that corner and marveled at the coincidence. What is the probability of this happening? she remembers wondering. What did this mean?

"How stupid we were," Falk says now, "to be so surprised. We related to all the details that had converged to create that moment. But the real question was what was the probability that at some time in some place I would meet one of my circle of friends? And when I told this story to others at work, they encoded the events as two Israelis meeting in New York, something that happens all the time."

Why was her experience so resonant for her, Falk asked herself, but not for those around her? One of the many experiments she has conducted since then proceeded as follows: she visited several large university classes, with a total of 200 students, and asked each student to write his or her birth date on a card. She then quietly sorted the cards and found the handful of birthdays that students had in common. Falk wrote those dates on the blackboard. April 10, for instance, Nov. 8, Dec. 16. She then handed out a second card and asked all the students to use a scale to rate how surprised they were by these coincidences.

The cards were numbered, so Falk could determine which answers came from respondents who found their own birth date written on the board. Those in

that subgroup were consistently more surprised by the coincidence than the rest of the students. "It shows the stupid power of personal involvement," Falk says.

The more personal the event, the more meaning we give it, which is why I am quite taken with my story of meeting my husband (because it is a pivotal moment in my life), and why SQuire Rushnell is also taken with it (because it fits into the theme of his book), but also why Falk is not impressed at all. She likes her own story of the chance meeting on a corner better than my story, while I think her story is a yawn.

The fact that personal attachment adds significance to an event is the reason we tend to react so strongly to the coincidences surrounding Sept. 11. In a deep and lasting way, that tragedy feels as if it happened to us all.

Falk's findings also shed light on the countless times that pockets of the general public find themselves at odds with authorities and statisticians. Her results might explain, for instance, why lupus patients are certain their breast implants are the reason for their illness, despite the fact that epidemiologists conclude there is no link, or why parents of autistic children are resolute in their belief that childhood immunizations or environmental toxins or a host of other suspected pathogens are the cause, even though experts are skeptical. They might also explain the outrage of all the patients who are certain they live in a cancer cluster, but who have been told otherwise by researchers.

Let's be clear: this does not mean that conspiracies do not sometimes exist or that the environment never causes clusters of death. And just as statistics are often used to show us that we should not be surprised, they can also prove what we suspect, that something is wrong out there.

"The fact that so many suspected cancer clusters have turned out to be statistically insupportable does not mean the energy we spent looking for them has been wasted," says Dr. James M. Robins, a professor of epidemiology and biostatistics at Harvard and an expert on cancer clusters. "You're never going to find the real ones if you don't look at all the ones that don't turn out to be real ones."

Most often, though, coincidence is a sort of Rorschach test. We look into it and find what we already believe. "It's like an archer shooting an arrow and then drawing a circle around it," Falk says. "We give it meaning because it does mean something—to us."

Vladimir Pasechnik was 64 when he died. His early career was spent in the Soviet Union working at Biopreparat, the site of that country's biological weapons program. He defected in 1989 and spilled what he knew to the British, revealing

for the first time the immense scale of Soviet work with anthrax, plague, tularemia and smallpox.

For the next 10 years, he worked at the Center for Applied Microbiology and Research, part of Britain's Department of Health. Two years ago, he left to form Regma Biotechnologies, whose goal was to develop treatment for tuberculosis and other infectious disease. In the weeks before he died, Pasechnik had reportedly consulted with authorities about the growing anthrax scare. Despite all these intriguing details, there is nothing to suggest that his death was caused by anything other than a stroke.

Robert Schwartz's death, while far more dramatic and bizarre, also appears to have nothing to do with the fact that he was an expert on DNA sequencing and analysis. On Dec. 10 he was found dead on the kitchen floor of his isolated log-and-fieldstone farmhouse near Leesburg, Va., where he had lived alone since losing his wife to cancer four years ago and his children to college. Schwartz had been stabbed to death with a two-foot-long sword, and his killer had carved an X on the back of his neck.

Three friends of Schwartz's college-age daughter were soon arrested for what the prosecutor called a "planned assassination"; two of the trials for first-degree murder are scheduled for this month. A few weeks later, police arrested the daughter as well. One suspect has a history of mental illness, and their written statements to police talk of devil worship and revenge. There is no talk, however, of microbiology.

On the same day that Schwartz died, Set Van Nguyen, 44, was found dead in an air-locked storage chamber at the Australian Commonwealth's Scientific and Industrial Research Organisation's animal diseases facility in Geelong. A months-long internal investigation concluded that a string of equipment failures had allowed nitrogen to build up in the room, causing Nguyen to suffocate. Although the center itself dealt with microbes like mousepox, which is similar to smallpox, Nguyen himself did not. "Nguyen was in no way involved in research into mousepox," says Stephen Prowse, who was the acting director of the Australian lab during the investigation. "He was a valued member of the laboratory's technical support staff and not a research scientist."

Word of all these deaths (though not the specific details) found its way to Ian Gurney, a British writer. Gurney is the author of *The Cassandra Prophecy: Armageddon Approaches*, a book that uses clues from the Bible to calculate that Judgment Day will occur in or about the year 2023. He is currently researching his

second book, which is in part about the threat of nuclear and biological weapons, and after Sept. 11 he entered a news alert request into Yahoo, asking to be notified whenever there was news with the key word "microbiologist."

First Que, then Wiley, then Pasechnik, Schwartz and Nguyen popped up on Gurney's computer. "I'm not a conspiracy theorist," says the man who has predicted the end of the world, "but it certainly did look suspicious." Gurney compiled what he had learned from these scattered accounts into an article that he sent to a number of Web sites, including Rense.com, which tracks U.F.O. sightings worldwide. "Over the past few weeks," Gurney wrote, "several world-acclaimed scientific researchers specializing in infectious diseases and biological agents such as anthrax, as well as DNA sequencing, have been found dead or have gone missing."

The article went on to call Benito Que, the cancer lab technician, "a cell biologist working on infectious diseases like H.I.V.," and said that he had been attacked by four men with a baseball bat but did not mention that he suffered from high blood pressure. It then described the disappearance of Wiley without mentioning his seizure disorder and the death of Pasechnik without saying that he had suffered a stroke. It gave the grisly details of Schwartz's murder, but said nothing of the arrests of his daughter's friends. Nguyen, in turn, was described as "a skilled microbiologist," and it was noted that he shared a last name with Kathy Nguyen, the 61-year-old hospital worker who just happened to be the one New Yorker to die of anthrax.

Of course, there have always been rumors based on skewed historical fact. Recall, for example, the list of coincidences that supposedly linked the deaths of Presidents Lincoln and Kennedy. It goes, in part, like this: The two men were elected 100 years apart; their assassins were born 100 years apart (in fact, 101 years apart); they were both succeeded by men named Johnson; and the two Johnsons were born 100 years apart. Their names each contain seven letters; their successors' names each contain 13 letters; and their assassins' names each contain 15 letters. Lincoln was shot in a theater and his assassin ran to a warehouse, while Kennedy was shot from a warehouse and his assassin ran to a theater. Lincoln, or so the story goes, had a secretary named Kennedy who warned him not to go to the theater the night he was killed (for the record, Lincoln's White House secretaries were named John Nicolay and John Hay, and Lincoln regularly rejected warnings not to attend public events out of fear for his safety, including his own inauguration); Kennedy, in turn, had a secretary named Lincoln (true, Evelyn

Lincoln) who warned him not to go to Dallas (he, too, was regularly warned not to go places, including San Antonio the day before his trip to Dallas).

I first read about these connections five years after the Kennedy assassination, when I was 8, which says something about how conspiracy theory speaks to the child in all of us. But it also says something about the technology of the time. The numerological coincidences from the World Trade Center that I mentioned at the start of this article made their way onto my computer screen by Sept. 15, from a friend of a friend of a friend of an acquaintance, ad infinitum and ad nauseam.

Professor Robins of Harvard points out that "the Web has changed the scale of these things." Had there been a string of dead scientists back in 1992 rather than 2002, he says, it is possible that no one would have ever known. "Back then, you would not have had the technical ability to gather all these bits and pieces of information, while today you'd be able to pull it off. It's well known that if you take a lot of random noise, you can find chance patterns in it, and the Net makes it easier to collect random noise."

The Gurney article traveled from one Web site to the next and caught the attention of Paul Sieveking, a co-editor of *Fortean Times*, a magazine that describes itself as "the Journal of Strange Phenomena."

"People send me stuff all the time," Sieveking says. "This was really interesting." Wearing his second hat as a columnist for *The Sunday Telegraph* in London, he wrote a column on the subject for that paper titled "Strange but True—The Deadly Curse of the Bioresearchers." His version began with the link between the two Nguyens and concluded, "It is possible that nothing connects this string of events, but . . . it offers ample fodder for the conspiracy theorist or thriller writer."

Commenting on the story months later, Sieveking says: "It's probably just a random clumping, but it just happens to look significant. We're all natural storytellers, and conspiracy theorists are just frustrated novelists. We like to make up a good story out of random facts."

Over the months, Gurney added names to his list and continued to send it to virtual and actual publications around the U.S. Mainstream newspapers started taking up the story, including an alternative weekly in Memphis, where interest in the Wiley case was particularly strong, and most recently the *Toronto Globe and Mail*. The tally of "microbiologists" is now at 11, give or take, depending on the story you read. In addition to the men already discussed, the names that appear most often are these: Victor Korshunov, a Russian expert in intestinal bacteria,

who was bashed over the head near his home in Moscow; Ian Langford, a British expert in environmental risk and disease, who was found dead in his home near Norwich, England, naked from the waist down and wedged under a chair; Tanya Holzmayer, who worked as a microbiologist near San Jose and was shot seven times by a former colleague when she opened the door to a pizza delivery man; David Wynn-Williams, who studied microbes in the Antarctic and was hit by a car while jogging near his home in Cambridge, England; and Steven Mostow, an expert in influenza, who died when the plane he was piloting crashed near Denver.

The stories have also made their way into the e-mail in-boxes of countless microbiologists. Janet Shoemaker, director of public and scientific affairs for the American Society for Microbiology, heard the tales and points out that her organization alone has 41,000 members, meaning that the deaths of 11 worldwide, most of whom were not technically microbiologists at all, is not statistically surprising. "We're saddened by anyone's death," she says. "But this is just a coincidence. In another political climate I don't think anyone would have noticed."

Ken Alibek heard them, too, and dismissed them. Alibek is one of the country's best-known microbiologists. He was the No. 2 man at Biopreparat (where Victor Pasechnik also worked) before he defected and now works with the U.S. government seeking antidotes for the very weapons he developed. Those who have died, he says, did not really know anything about biological weapons, and if there were a conspiracy to kill scientists with such knowledge, he would be dead. "I considered all this a little artificial, because a number of them couldn't have been considered B.W. experts," he says with a hint of disdain. "I got an e-mail from Pasechnik before he died, and he was working on a field completely different from this. People say to me, 'Ken, you could be a target,' but if you start thinking about this, then your life is over. I'm not saying I'm not worried, but I'm not paying much attention. I'm opening my mail as usual. If I see something suspicious, I know what to do."

Others are not quite as sanguine. Phyllis Della-Latta is the director of clinical microbiology services at New York's Columbia Presbyterian Medical Center. She found an article on the deaths circulating in the most erudite place—an Internet discussion group of directors of clinical microbiology labs around the world. These are the people who, when a patient develops suspicious symptoms, are brought in to rule out things like anthrax.

Della-Latta, whom I know from past medical reporting, forwarded the article to me with a note: "See attached. FYI. Should I be concerned??? I'm off on a

business trip to Italy tomorrow & next week. If I don't return, write my obituary."

She now says she doesn't really believe there is any connection between the deaths. "It's probably only coincidence," she says, then adds: "But if we traced back a lot of things that we once dismissed as coincidence—foreigners taking flying lessons—we would have found they weren't coincidence at all. You become paranoid. You have to be."

Don Wiley's body was finally found on Dec. 20, near Vidalia, La., about 300 miles south of where he disappeared.

The Memphis medical examiner, O.C. Smith, concluded that yellow paint marks on Wiley's car suggest that he hit a construction sign on the Hernando DeSoto Bridge, as does the fact that a hubcap was missing from the right front tire. Smith's theory is that heavy truck traffic on the bridge can set off wind gusts and create "roadway bounce," which might have been enough to cause Wiley to lose his balance after getting out of the car to inspect the scrapes. He was 6-foot-3, and the bridge railing would have only come up to mid-thigh.

"If Dr. Wiley were on the curb trying to assess damage to his car, all of these factors may have played a role in his going over the rail," Smith said when he issued his report. Bone fractures found on the body support this theory. Wiley suffered fractures to his neck and spine, and his chest was crushed, injuries that are consistent with Wiley's hitting a support beam before he landed in the water.

The Wiley family considers this case closed. "These kinds of theories are something that's always there," says Wiley's wife, Katrin Valgeirsdottir, who has heard all the rumors. "People who want to believe it will believe it, and there's nothing anyone can say."

The Memphis police also consider the case closed, and the local office of the F.B.I. has turned its attention to other odd happenings. The talk of Memphis at the moment is the bizarre ambush of the city's coroner last month. He was wrapped in barbed wire and left lying in a stairwell of the medical examiner's building with a live bomb strapped to his chest.

Coincidentally, that coroner, O.C. Smith, was also the coroner who did the much-awaited, somewhat controversial autopsy on Don Wiley.

What are the odds of that?

August 11, 2002

Fractal Vision

By JAMES GLEICK

Here is a mathematician's nightmare I heard in the 1980s when that irritating, unconforming, self-regarding provocateur Benoît Mandelbrot was suddenly famous—fractals, fractals everywhere. The mathematician dreamed that Mandelbrot died, and God spoke: "You know, there really was something to that Mandelbrot."

Sure enough.

Mandelbrot created nothing less than a new geometry, to stand side by side with Euclid's—a geometry to mirror not the ideal forms of thought but the real complexity of nature. He was a mathematician who was never welcomed into the fraternity ("Fortress Mathematics," he said, where "the highest ambition is to wall off the windows and preserve only one door"), and he pretended that was fine with him. When Yale first hired him to teach, it was in engineering and applied science; for most of his career he was supported at I.B.M.'s Westchester research lab. He called himself a "nomad by choice." He considered himself an experienced refugee: born to a Jewish family in Warsaw in 1924, he immigrated to Paris ahead of the Nazis, then fled farther and farther into the French countryside.

In various incarnations he taught physiology and economics. He was a non-physicist who won the Wolf Prize in physics. The labels didn't matter. He turns out to have belonged to the select handful of 20th-century scientists who upended, as if by flipping a switch, the way we see the world we live in.

He was the one who let us appreciate chaos in all its glory, the noisy, the wayward and the freakish, from the very small to the very large. He gave the new field of study he invented a fittingly recondite name: "fractal geometry." But he wanted me to understand it as ordinary.

"The questions the field attacks are questions people ask themselves," he told me. "They are questions children ask: What shape is a mountain? Why is a cloud the way it is?" Only his answers were not ordinary.

Clouds are not spheres—the most famous sentence he ever wrote—mountains are not cones, coastlines are not circles and bark is not smooth, nor does lightning travel in a straight line.

If you closely examine the florets of a cauliflower (or the bronchioles of a lung;

or the fractures in oil-bearing shale), zooming in with your magnifying glass or microscope, you see the same fundamental patterns, repeating. It is no accident. They are all fractal. Clouds, mountains, coastlines, bark and lightning are all jagged and discontinuous, but self-similar when viewed at different scales, thus concealing order within their irregularity. They are shapes that branch or fold in upon themselves recursively.

I was following him from place to place, reporting a book on chaos, while he evangelized his newly popular ideas to scientists of all sorts. Wisps of white hair atop his outsize brow, he lectured at Woods Hole to a crowd of oceanographers, who had heard that fractals were relevant to cyclone tracks and eddy cascades. Mandelbrot told them he had seen the same channels, flows and back flows in dry statistics of rising and falling cotton prices. At Lamont-Doherty Geological Observatory, as it was then known, the geologists already spoke fractally about earthquakes. Mandelbrot laid out a mathematical framework for such phenomena: they exist in fractional dimensions, lying in between the familiar one-dimensional lines, two-dimensional planes and three-dimensional spaces. He revived some old and freakish ideas—"monsters," as he said, "mathematical pathologies" that had been relegated to the fringes.

"I started looking in the trash cans of science for such phenomena," he said, and he meant this literally: one scrap he grabbed from a Paris mathematician's wastebasket inspired an important 1965 paper combining two more fields to which he did not belong, "Information Theory and Psycholinguistics." Information theory connected to fractals when he focused on the problem of noise—static, errors—in phone lines. It was always there; on average it seemed manageable, but analysis revealed that normal bell-curve averages didn't apply. There were too many surprises—outliers. Clusters and quirks always defied expectations.

It's the same with brainwaves, fluid turbulence, seismic tremors and—oh, yes—finance.

From his first paper studying fluctuations in the rise and fall of cotton prices in 1962 until the end of his life, he maintained a simple and constant message about extraordinary economic events. The professionals plan for "mild randomness" and misunderstand "wild randomness." They learn from the averages and overlook the outliers. Thus they consistently, predictably, underestimate catastrophic risk. "The financiers and investors of the world are, at the moment, like mariners who heed no weather warnings," he wrote near the peak of the bubble, in 2004, in *The (Mis)behavior of Markets*, his last book.

Fractals have made their way into the economics mainstream, as into so many fields, though Mandelbrot was not really an economist; nor a physiologist, physicist, engineer. . . .

"Very often when I listen to the list of my previous jobs, I wonder if I exist," he said once. "The intersection of such sets is surely empty."

December 21, 2010



CHAPTER 5

Cryptography and the Emergence of Truly Unbreakable Codes

IN THOSE LONG AGO TIMES OF THE EARLY 1990s, BEFORE e-commerce was commonplace, before most people even thought about the problems of keeping data secret, of typing credit card numbers into Web sites and assuming they will be secure, the federal government and scientists engaged in an epic debate.

Mathematicians had devised a clever way to make coding systems that could not be compromised. The most popular relied on factoring large numbers—the idea behind it was that it was simple to multiply prime numbers together and get a huge composite number, but if all you had was the composite number, there was no feasible way to find the primes that make it up. There was the method of simply trying all the primes smaller than the composite, and there were a few shortcuts. But if the composite was big enough, it would simply be infeasible, even with the fastest computers, to break that composite down.

So encoding would, essentially, involve multiplying primes and using that method to encrypt a digital file. Decoding, for anyone who

did not know the primes, would be impossible because it would be so hard to find the original set of primes.

Mathematicians called these “one-way functions.” They were easy in one direction—multiply primes—and almost impossible in the other direction—find the primes that were multiplied.

Yet if the method was that good, the codes that unbreakable, did we really want the system to be public so anyone, including terrorists or enemy countries, could use it? The National Security Agency, which makes codes used by the federal government, including the military, and breaks codes used by other countries or terrorists, stepped in and asked to review mathematicians’ papers before they were published, lest they unintentionally reveal secrets and methods that could imperil the N.S.A.’s mission.

What ensued was a battle and a debate over how public this work should be and whether, once an idea is mentioned, it is even possible to prevent others from developing it.

The *Times* articles tell the story of the wrenching arguments and the research that ensued—attempts to find good ways of breaking large composite numbers into primes, attempts to probe the codes and see how good they really are. It is a story that still resonates, even as secure codes have become part of everyone’s life.

Harassment Alleged over Code Research

By MALCOLM W. BROWNE

Computer scientists and mathematicians whose research touches on secret codes say they have been subjected by the National Security Agency to growing harassment and the threat of sanctions or even prosecution for publishing articles about their work.

The scientists, some working for universities, some for private industry and some for the federal government, charge that research in the United States faces a muted but growing threat from the National Security Agency, the government's supreme authority on secret codes.

The agency's tactics, they say, may eventually mean that a scientist working outside the government could suddenly be informed that his work had been officially classified as secret, or he could even be constrained from participating in international professional meetings.

Norman Boardman, spokesman for the N.S.A., told *The New York Times* that neither he nor any other employee of the agency could comment in any way on the accusations made by the scientists.

Complaining scientists, lawyers for scientific institutions and government experts agree that laws covering such potential constraints are ambiguous. But because of the vagueness of the current legal position, the security agency's pressure must be taken seriously, they assert.

Prosecution Reported Threatened

Scientists said in interviews that threats leveled against them by employees of the agency included the possibility of official action to get research grants canceled or even criminal prosecution for violation of security laws.

A source within the National Science Foundation, a federal agency that underwrites many research programs by private organizations and individuals, said that his organization was being subjected to increasing "systematic, bureaucratic sniping" from the security agency with a view to bringing certain kinds of research under the agency's control.

The informant, who asked that his identity not be disclosed, said there was

a danger of intimidating a large segment of the private American scientific community if the government pressure was not resisted.

Such allegations have been simmering in the scientific press for about six months, but the controversy was brought to a boil by a symposium on information theory held last week at Cornell University at Ithaca, N.Y.

Among the scientists who presented papers at the meeting was a group from Stanford University headed by Dr. Martin E. Hellman and an associate, Whitfield Diffie.

The Stanford group had been concentrating its studies on a kind of mathematical problem known as the Nondeterministic Polynomial Complete Problem (N-P Complete).

A Computer "Lock"

The N-P Complete problem's special interest to computer scientists is that at this point no computer can be programmed to solve it. Dr. Hellman and his associates have therefore proposed it as a device for "locking" data in the memory banks of computers against unauthorized use or theft.

"The right to privacy of the American citizen is what this is all about," he said.

However, the N-P Complete problem could also be used as a system for devising secret communications codes that, Dr. Hellman contends, would also be virtually impossible to break, even by giant intelligence organizations, including the National Security Agency.

The implication, Dr. Hellman and others said, was that any government, private organization or individual could devise and use a code that would be immune to eavesdropping, whether from the Central Intelligence Agency, the Soviet Union's counterpart, the K.G.B., or any other group.

They, say the experts involved, created anxiety within the United States intelligence community. In an interview, a senior government intelligence official described the issues raised by the Hellman team as "extremely serious" to the national security interests of the country.

The Stanford work and related projects by the Massachusetts Institute of Technology and others, he said, could enable foreign powers to develop virtual impenetrable command-and-control military communications systems.

Most computer scientists and mathematicians in the United States are members of the Institute of Electric and Electronic Engineers, which publishes

their papers and distributes them to countries abroad, including the Soviet Union among other countries.

Letter Regarded as Threat

Several weeks before the Cornell conference, the institute received a letter from one of its members, Joseph A. Meyer, who is listed, well-placed scientists say, in the National Security Agency directory as an employee.

The letter warned the Institute that publication and distribution of scientific papers by the Stanford team and other groups planning to participate in the Cornell conference could result in prosecution under the 1954 Munitions Control Act, known in its current revision as the Arms Export Control Act.

Lawyers of the institute studied Mr. Meyer's letter and the law itself, and finally concluded that they were within the law in publishing the Stanford research. A similar view was taken by lawyers representing Stanford University and officials interviewed by *The New York Times* in the Department of Commerce, the agency responsible for issuing licenses for exported technology.

Denial by Security Agency

Mr. Boardman, the security agency spokesman, denied that the N.S.A. had directed any employee to bring pressure on Mr. Hellman or the others. But an informant in the National Science Foundation said the letter from Mr. Meyer to the engineering institute was merely one of a number of similarly threatening letters that had been sent to scientists and their organizations by known employees of the security agency.

Efforts by *The New York Times* to reach Mr. Meyer at his home in Bethesda, Md., or at his N.S.A. office at Fort Meade, Md., were not successful. Telephone calls were referred to the N.S.A. spokesman, who declined comment.

October 19, 1977

Researchers to Permit Pre-Publication Review by U.S.

By RICHARD SEVERO

A group of mathematicians and computer scientists has tentatively decided to try to dispel a concern of the National Security Agency by voluntarily submitting research papers to the agency for review before they are published in the scientific literature.

The National Security Agency, which has the responsibility for collecting intelligence information, is concerned because, it says, cryptographic research in universities has become so advanced in recent years that it is viewed as a security hazard. Until a few years ago the government had a virtual monopoly on such research.

Cryptography, the art of writing or deciphering messages in code, has increasingly become a focus of academic interest, in great measure because of the need to protect industrial secrets. There is said to be apprehension within the National Security Agency over whether an academic researcher might write a paper on methods of analytically attacking and breaking a code system similar to one used by the government.

The decision to attempt to cooperate with the agency without violating the tradition of academic freedom was made at a recent meeting of the Public Cryptography Study Group. Details of the precise form the cooperation will take, beyond allowing agency review, have not been formulated.

Concern about Possible Controls

The group was set up last year by the American Council on Education, which is made up of university administrators. The study group itself is nine members representing professional societies in computer sciences and mathematics. It does not represent all cryptographers, and some remain acutely concerned that the cooperation may become the first phase of federal control over cryptography in American universities.

Daniel Schwartz, general counsel of the agency, said yesterday that nothing of the sort was contemplated. Asked what the government would do if the voluntary program did not work, Mr. Schwartz said the agency "would consider as

one option seeking legislation if the problem became serious enough and there was no other way to resolve it."

But he emphasized the agency considered such an action a last resort and added: "We have no interest in going through an enormous fight in the Congress on this particular issue." He said the agency would probably not object to most papers and if it did, the problem might be resolved by the deletion of an explanatory footnote.

Conflict concerning Financing

Dr. Ronald Rivest, a computer scientist at the Massachusetts Institute of Technology, said he thought the study group's recommendations might be workable. "But I think it is important not to forget that the need for any sort of recommendations has not been made to anybody's satisfaction outside of the National Security Agency," Dr. Rivest added.

He was asked how he would feel about the financing of his work by the agency. Agency financing of academic research has been a disputed issue in recent years.

"I feel it is institutionally inappropriate," he said. "There would be a conflict of principles within the National Security Agency. On the one hand it would be concerned with maintaining national security, and on the other hand it would be concerned with maintaining the principle of open and academic research."

Dr. Martin Hellman, professor of electrical engineering at Stanford University, said he was also ready to try to cooperate. "If it doesn't work," he said, "we can back off." Dr. Hellman said he thought the agency had become easier to work with in recent years.

The relationship between academic cryptographers and the agency became a matter of some controversy last August when Leonard Adleman, a computer scientist at M.I.T. and at the University of Southern California, learned that the National Science Foundation had passed his research proposal along to the National Security Agency, which then approached him about the possibility of providing some funds.

Dr. Adleman said he wanted no money from the agency. Since then he has been allowed to re-apply for money from the National Science Foundation.

November 1, 1980

Tighter Security Rules for Advances in Cryptology

By WALTER SULLIVAN

The Japanese Navy was defeated in World War II largely because American code-breakers had deciphered Japanese intentions before the pivotal Battle of Midway. Cryptography played a key role several other times in that war.

Today, however, it is confronted with a two-edged crisis, and there is some doubt that it will ever play so significant a role again. Some specialists believe that thanks to computers, cryptography has become so impenetrable that the days when great powers could "read each other's mail" may be nearing an end. At the same time, as interlocking computer networks proliferate, secure coding systems are becoming essential to safeguard the national economy, individual businesses and personal privacy.

These developments have led to a confrontation between the National Security Agency, responsible for deciphering the communications of other nations and safeguarding those of the United States, and academic specialists seeking to meet the needs of the private sector. Although a voluntary compromise has been reached, it is unclear how wide the compliance will be.

Some academicians contend that increased federal control of their work will have a "chilling effect." Officials of the security agency fear that public disclosure of coding systems that are increasingly difficult to break will give away its secrets or enable foreign powers to frustrate American code-breaking efforts.

The Background

In 1976, Martin E. Hellman of Stanford University and his colleagues, Whitfield Diffie and Ralph Merkle, conceived a "public key" approach to cryptography, in which one key that can be made public is used to encode the information and a second key, kept secret, is needed to decipher it.

At the Massachusetts Institute of Technology, Ronald L. Rivest, Adi Shamir and Leonard Adleman then proposed a system employing the "public key" approach. Known as the R.S.A. system, it is widely regarded as unbreakable, given present computer capabilities.

In this system the message can be typed into a computer that converts it into

numbers and alters them, using a special mathematical key. The recipient must use another key to retrieve the original numbers and text. To reverse the encoding process without the deciphering key, it is said, would require computer processing lasting thousands or even billions of years.

When officials of the National Security Agency learned of these developments, they feared that the academic community was arming foreign cryptographers with ways to foil its deciphering efforts. They sought to take over from the National Science Foundation the awarding of some research grants in this area, including one sought by Dr. Adleman. The agency also asked the Federal Patent Office to impose secrecy classification on some encoding or voice-scrambling devices intended for commercial use, including one developed by Dr. George I. Davida of the University of Wisconsin.

Last year, in response to a suggestion by Vice Adm. Bobby R. Inman, then the director of the security agency, the American Council on Education formed a Public Cryptography Study Group to explore the situation. Dr. Hellman and Dr. Davida were members of the study group.

For Control

Two years ago, as reported by the study group in February, Admiral Inman "publicly indicated his deep concern that some information contained in published articles and monographs on cryptography endangered the mission of N.S.A. and thus the national security." Admiral Inman, who was succeeded by Lieut. Gen. Lincoln Faurer of the Air Force, favored some form of legislated control.

It was argued that foreign powers were aided by the publication of such material as the detailed accounts of public-key cryptography that appeared in *Transactions of the Institute of Electrical and Electronic Engineers* and then in *Scientific American*.

Although some scientists always voluntarily offer their work for review, the security agency cannot require that reports be submitted to it for approval, unless the agency has financed the work. The National Science Foundation refers sensitive information developed under its grants to the security agency or to the intelligence officials of one of the armed forces.

One suggested way to achieve the control sought by the security agency would be to make it a crime to reveal sensitive cryptologic information as defined in a statute. Another approach would be to require prepublication

review. Compensation would be paid those who suffered financial loss when their invention was made secret.

Against Control

The nation is becoming increasingly vulnerable to clandestine penetration of its computer networks. Information of commercial value can be extracted without leaving any evidence of the theft. Money transactions can be manipulated in subtle forms of embezzlement. Personal privacy can be invaded.

According to Michael Dertouzos, director of M.I.T.'s Laboratory for Computer Science, hostile agents could cause chaos by putting false information in the computers that control the nation's monetary system. Such hazards could be avoided by the use of cryptographic methods to protect legitimate information and authenticate additions.

It has been argued that development and introduction of such methods in the private sector was more important to the nation than concealing them from foreign cryptographers. Dr. Adleman even suspects that such advanced countries as the Soviet Union are already using codes that cannot be broken by any foreseeable methods.

Dr. Davida, however, is less certain of this. Methods like the public key system are not intrinsically undecipherable. There is always the possibility that someone will find a shortcut to its solution, he says. He doubts that cryptography will become so undecipherable that the role of the security agency will become obsolete.

Dissent on Papers

As a member of the study group, Dr. Davida was the sole dissenter from its recommendation for voluntary submission of cryptography papers to the security agency. Computer nets, he wrote, constitute "electronic windows into the most intimate details of people's lives." Even more disturbing, he added, "is that it is usually impossible to know who is looking in." Encryption can serve as a curtain.

In a reference to the American Telephone and Telegraph Company, as well as other communications companies, he said the need for such curtains, "is crystal clear in view of the remarkable insensitivity of the common carriers to the

public's concern about privacy." Dr. Dertouzos opposes any control over academic research. "A university, to be effective, has to be free," he said in a recent interview. "We are responsible people." Like many of those working in this field, he sends his papers to the National Security Agency. He says, however, that this is "for information only," not for clearance.

Dr. Hellman said that if he was persuaded that publication of a paper would hinder the operations of the security agency more than it would aid the private sector he would be willing to withhold it.

The Outlook

The study group, on which the security agency was represented by its general counsel, Daniel C. Schwartz, has agreed to a compromise, voluntary arrangement for a trial period. Under the procedure, which so far has won only limited acceptance in the academic community, the security agency would define the nature of papers it wished to review and "invite" their submission. If its recommendations were not accepted by the author, the issue would be referred to a five-member advisory committee.

Two of the advisory panel's members would be from the security agency and three nominated by the president of the National Academy of Sciences. The procedure is just getting under way. Formation of the committee will be time-consuming because of the need to obtain security clearances for those members not representing the security agency.

Each researcher or academic institution will be faced with a decision. If this procedure wins wide compliance it may serve the security agency's needs. On the other hand, it may prove ineffective if even a few sensitive papers are not submitted for screening.

June 1, 1981

A New Approach to Protecting Secrets Is Discovered

By JAMES GLEICK

Mathematicians and cryptologists have discovered a way for people to prove that they possess secret information—from their credit card numbers to military access codes—without giving any of the information away.

This keenly paradoxical discovery has upset the traditional understanding of mathematical proof. Beyond that, however, it may also hold the power to transform the many aspects of modern life where processes of identification are subject to abuse, from everyday financial transactions to encounters between enemy aircraft.

Blending pure logic with computer technology, the researchers are developing an area of mathematics called zero-knowledge proof. Where a conventional proof conveys information, a zero-knowledge proof is meant to convey only the assurance that the information is in hand. The goal is to convince a second party without providing any of the knowledge that would allow him, or an eavesdropper, to convince a third party.

"You want to be able to prove some fact and not disclose why the fact is true," said Silvio Micali of the Massachusetts Institute of Technology, one of the originators of the idea. "You want to convince without giving more knowledge than is strictly necessary." Ideally, that is no knowledge at all.

Although zero-knowledge proof began as an abstraction, computer scientists quickly realized its applicability to many everyday uses of secrecy. The issue arises whenever someone tears up credit-card carbons, looks over his shoulder while signing onto a computer or worries about the photocopying of a passport left with a hotel concierge.

"Everybody has secret information that he needs to show to somebody to identify himself," said Adi Shamir of Israel's Weizmann Institute of Science. With zero-knowledge proofs, "instead of giving away the secret, he proves he knows the secret," he said.

Dr. Shamir and two co-workers, Amos Fiat and Uriel Feige, have designed a way to use zero-knowledge proof cheaply and quickly in electronic chips that could be implanted, for example, in credit cards. Credit cards using chips, "smart cards," are already in development, but a smart card using zero-knowledge proof could

identify the cardholder to a merchant without giving the merchant the knowledge—the card number—that would let him make illicit purchases or forge a new card.

"I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me," Dr. Shamir said. Because this invention also affects military uses of identification procedures, the United States recently imposed a secrecy order on it; the order was quickly rescinded amid an outcry from American mathematicians. The fundamental mathematical ideas of zero-knowledge proof that underlie the invention are firmly in the public domain, and many researchers are pursuing other applications.

The essence of zero-knowledge proof lies in an interactive exchange of information between the "prover" and the "verifier." That is a break with the traditional practice of simply writing a proof down, once and for all—or simply revealing one's password.

"What I find most exciting is that the whole notion of what constitutes a mathematical proof is broadening," said Manuel Blum of the University of California at Berkeley, who has played a central role in making such proofs workable. "This interactive exchange has never existed before. In Euclid the proofs are written down—from Euclid to us—just one way."

The other new element is a role for chance. In effect, the verifier asks a series of questions, choosing the questions by some electronic equivalent of flipping a coin.

Suppose, for example, the prover has a bafflingly complex maze the size of New York City. She points to two locations—Times Square and Shea Stadium—and asserts that she knows paths through the maze connecting them. How can she convince a verifier without actually showing him how to get from one point to the other?

Process of Interrogation

She picks a third point on a path—say, the Brooklyn Promenade—and offers to reveal either the path from Times Square to the promenade or the path from the promenade to the stadium. The verifier flips a coin and chooses one half-path or the other. If she is lying, he already has a 50 percent chance of catching her.

Now she picks yet another point—Rikers Island—and they repeat the process of interrogation. The verifier checks either the path from Times Square to Rikers or from Rikers to the stadium. Again, if the prover is lying, she has a 50 percent chance of being caught.

"Eventually you are convinced, because of my willingness to show you either of two halves," Dr. Shamir said. "You chose which half you wanted to see."

The verifier can repeat the process as long as he likes. After 300 inquiries, the chance that she is lying has fallen to one part in 2^{300} , more than the number of atoms in the universe.

This example is not quite a zero-knowledge proof, however. Even though the verifier never actually sees a full path, the many fragments of paths can eventually enable him to piece together an understanding of the maze.

A more precise example involves a collection of lines joined at nodes, which mathematicians call a graph. A well-known problem is to ask whether it is possible to paint the nodes of a certain graph, using just three different colors, so that no line has the same color at both ends.

To construct a large graph that can be colored this way is easy. But the reverse problem, to find a way of coloring a given graph, has been shown to be very hard—a member of a class of problems that cannot be solved in a reasonable amount of time. The difficulty of the problem rises rapidly as the graph becomes bigger.

Practical Applications

Dr. Micali and other experts in the field, who include Shafi Goldwasser, Charles Rackoff, Oded Goldreich and Avi Wigderson, have shown that graph colorings—and all other problems in the same hard class—can be proved in ways that convey zero knowledge of the proof.

Similar problems of pure mathematics are used electronically in the practical applications. Instead of a credit-card number, a user may have a computer chip containing, in effect, a unique, complicated graph and its coloring. A verifying computer knows the graph associated with each user, but does not know how to color it.

For practical applications, the mathematics of graph coloring are too slow. But using techniques of number theory, researchers have come up with zero-knowledge proofs that adapt well to electronic circuitry. Dr. Shamir's device carries out the whole back-and-forth exchange in less than one second.

"It's about 100 times faster," he said. "If you had to wait 100 seconds for a smart card to prove its identity, no one would use such a scheme."

Most important to many applications is that the technology of zero-knowledge proof so effectively separates the ability to generate a proof from the ability to verify it.

Protecting Aircraft Signals

That addresses a security problem that arises in the most sensitive areas. For example, "friend or foe" recognition signals used by military aircraft can, in theory, be intercepted electronically or analyzed from captured aircraft. A system based on zero-knowledge proof would be impervious to both threats, mathematicians suggest.

The same applies to emergency destruct signals sent in encoded form from ground controllers to missiles. By separating the ability to generate an identification from the ability to verify the identification, a system would remain secure even when missiles with their electronics were captured and examined.

"There are going to be thousands of those boxes in missiles to verify those instructions, and it's going to be very difficult to keep the secrecy of the verification device," said one researcher. "It's going to be much easier to keep the secrecy of the instruction-generation device that's going to be stored in the basement of the White House."

As the technology advances, however, the less apocalyptic applications will come first. Some mathematicians speculate about automated procedures for signing contracts or communicating orders to stockbrokers.

Signing on to Computers

It may even be possible for users to dispense with the electronics. Dr. Blum is designing a procedure for signing onto computer systems that would remove the possibility of intercepting a password. He envisions users being presented with a string of about 10 letters, and typing a response of the same length—but a different response every time.

In effect, the sequence of letters is like a sequence of 10 questions to the user, and the "password" is actually a procedure for changing some letters to others. For the system to work, the procedure has to be so easy that no calculation will be involved.

"But somebody who's watching you won't be helped a bit," Dr. Blum said, "because when he tries to log on as you, he'll be asked different questions."

February 17, 1987

Brief U.S. Suppression of Proof Stirrs Anger

No one at Israel's Weizmann Institute of Science knew more about secrets than Adi Shamir.

Nevertheless, Dr. Shamir, one of the world's best-known cryptologists, was caught off guard last month when the United States imposed a blanket secrecy order on a breakthrough he had made in the rapidly expanding mathematical field of zero-knowledge proofs. Declaring the Israeli work "detrimental to the national security" and warning of penalties that included imprisonment, the government ordered Dr. Shamir and his co-workers to recover and destroy all related material.

Within days, as the order began to cause a public furor among American mathematicians, the government agreed to reverse its action on the narrow ground that secrecy orders may not be imposed on the work of foreigners.

The incident has alarmed some mathematicians, who say they consider it an unusual and potentially harmful effort by the government to block the dissemination of a theoretical advance in science. In its aftermath, they see it as a threat to an uneasy working relationship that has developed over the last six years between mathematicians and the National Security Agency.

"I think it's a farce," Zvi Galil, a Columbia University mathematician and computer scientist, said as the incident began to develop. "It was already a concession from the scientists to agree to a review process giving some power to these guys from N.S.A."

Math and Cryptography

Officials of the Army, which requested the order, and the Patent and Trademarks Office, which issued it Jan. 6, describe it as a simple mistake and say that, to their knowledge, the highly secretive National Security Agency had no part in the decision.

The agency would not comment publicly, but one official said it had been "blind-sided." That was also the impression the agency sought to convey privately to many mathematicians.

The relationship between the nation's security agencies and mathematicians goes back many decades, but it has never been so intimate as it is today. Modern cryptography has become inseparable from the abstract development of

mathematics, and advances in many corners of mathematics can prove to have sensitive application to encoding and decoding information.

The N.S.A., believed to be the world's largest employer of mathematicians, has the delicate and sometimes irreconcilable missions of improving its own coding techniques while not giving foreign countries the ability to keep their communications secure from American decryption. The agency—sometimes known as No Such Agency—thrives on secrecy, and the number of mathematicians who work for it far exceeds the number who say they do.

The Shamir incident began after the Weizmann Institute, Israel's major civilian research center, applied last July for an American patent titled "Method, Apparatus and Article for Identification and Signature." The application described "unforgeable ID cards" based on the breakthrough by Dr. Shamir and two colleagues in zero-knowledge proofs, which allow a person to prove that he possesses sensitive information without actually revealing any of the information.

"That Word Military"

The application cited "numerous commercial and military applications."

As a result, the application was sent to the Army. "That word military automatically kicked it into the system," said Patricia Ann James of the Army's Legal Services Agency. After experts at Fort Belvoir in Virginia reviewed the matter, she put through the secrecy order on the ground that the research, though unclassified, belonged on the military critical technology list.

While the Army was studying the application, Dr. Shamir was describing the work at conferences in the United States and Europe, and written material was circulating among mathematicians. He was scheduled to present a full version in May at a major computer science conference to be held in New York, and he had submitted a paper to be published in connection with the conference.

After receiving the secrecy order and consulting with the Weizmann Institute's lawyers, Dr. Shamir formally notified the conference organizers that the paper could not be published. All copies of the preliminary papers in the hands of scientists or libraries "must be promptly destroyed," he told them.

The conference organizers considered halting publication. "Clearly I don't want to jeopardize the conference, and I wish to abide by the law," said Alfred Aho, a computer scientist who is program chairman for the conference. "But it

seems to me that this is rather outrageous that the United States government is trying to put a clamp of secrecy on this work."

Some mathematicians called the National Security Agency to register their objections.

To the patent office, the secrecy order may have seemed routine. Several hundred such orders are issued each year. But to mathematicians, it recalled a furor that broke out in 1977 when a secrecy order was imposed on an encryption device invented by George Davida, a professor at the University of Wisconsin. That order—also ultimately rescinded—helped lead to the current system of voluntary cooperation with the National Security Agency.

Under this system, many mathematicians submit copies of technical papers to the agency before publication, giving the agency an opportunity to request the suppression of sensitive material. Not all mathematicians abide by the arrangement, seeing it as a threat to the free exchange of ideas on which research depends. But many mathematicians believe that the government's security concerns are significant and that the bargain is a fair one. Many universities and corporate research departments cooperate with the N.S.A., as does the National Science Foundation.

"Tricky and Delicate"

"It's tricky and it's delicate and so far it's worked well," said Dr. Ronald L. Rivest of the Massachusetts Institute of Technology, one of the architects of the arrangement, along with Adm. Bobby R. Inman, then the agency's director.

Since 1980, the result has been a softening of tensions, which is one reason mathematicians were concerned about the new secrecy order. "It turns out that N.S.A., which several years ago were the bad guys, now are not the bad guys," Dr. Galil said.

Even foreign mathematicians tend to comply. In fact, according to several of those involved, Dr. Shamir submitted his latest breakthrough to the agency and it made no objection.

Soon after mathematicians began protesting to the agency, and within hours of inquiries by a newspaper reporter, the patent office said it would reverse the secrecy order. Some of those involved suggest that the agency had intervened forcefully behind the scenes. The agency would not say.

February 17, 1987

A Most Ferocious Math Problem Tamed

By MALCOLM W. BROWNE

By piecing together the output of hundreds of computers on three continents, a team of mathematicians succeeded yesterday in solving a monster computational problem that had defied all previous efforts. The achievement is likely to force cryptographers to reassess the future application of some codes used by governments and banks.

At 2:03 a.m., Pacific daylight time, the last sequence of numbers required for the solution popped up in a computer laboratory in Palo Alto, Calif., and news of the triumph was flashed to collaborators around the world. The team had succeeded for the first time in splitting a number 100 digits long into two large, prime factors.

The factors of a number are smaller numbers which, when multiplied by each other, yield the larger number. A prime number is one that is evenly divisible only by one or by itself. The prime factors of 15, for example, are 3 and 5.

Maximum Possible Difficulty

The two factors found for the 100-digit number, which was selected by an elaborate mathematical screening process to pose the maximum possible difficulty, are respectively 41 digits and 60 digits long.

The organizers of the project were Dr. Mark S. Manasse of the Digital Equipment Corporation's Systems Research Center in Palo Alto and Dr. Arjen K. Lenstra of the University of Chicago. But a dozen users of some 400 computers in the United States, the Netherlands and Australia were recruited to join in the project, donating computing time from intervals when the computers were not needed for their regular work.

Several of the most secure cipher systems invented in the past decade are based on the fact that large numbers are extremely difficult to factor, even using the most powerful computers for long periods of time. The accomplishment of factoring of a 100-digit number "is likely to prompt cryptographers to reconsider their assumptions about cipher security," Dr. Lenstra said in a telephone interview.

"We Have Upped the Ante"

His colleague, Dr. Manasse, added: "What this shows is that a cryptographer should avoid basing a cipher on any factorable number smaller than about 200. The cipher system still works, but we have upped the ante." Using larger numbers makes the work of cryptographers more cumbersome and time-consuming.

One cryptographic system based on the difficulty of factoring large numbers was invented in 1977 by Ronald L. Rivest, Adi Shamir and Leonard Adleman, all of the Massachusetts Institute of Technology. The three mathematicians patented their system and now market computer chips especially designed to apply it. In this and similar systems, digits replace each letter in a text message, and the entire sequence of digits is treated as a single large number. A mathematical operation is then performed on this number, and to decipher the result requires either that the receiver possesses the key or breaks the code by factoring the large number.

This kind of cipher system is regarded as too slow and cumbersome for such routine cipher messages as those used for secret government messages and the transfer of funds between banks. But according to Dr. Ron Graham, a mathematician at A.T.&T. Bell Laboratories, the "R.S.A. System" (which takes its initials from the names of its inventors) is used fairly extensively for the secure transmission of encryption and decryption keys from one organization to another.

Guarding Secret Keys

Encryption and decryption keys must be protected more securely than any other secret message, because these are the keys that allow either the intended recipient of a cipher message or a spy to decipher it. Since such a key is relatively short, the slowness of encrypting and decrypting it is a disadvantage more than offset by the method's relative security.

The R.S.A. method can accommodate factorable numbers of virtually any length as cipher keys, so yesterday's achievement does not compromise the method itself.

"Even if a user were to adopt a key 100 digits long," Dr. Manasse said, "it would take a gigantic organization working with single-minded dedication to accomplish what our network has done. I doubt that any organization using this kind of cipher is seriously worried by what we have done."

Potential of Supercomputer

Theoretically, a costly supercomputer such as the Cray, operating continuously, could have solved the problem in about one week, an expert said. But running such supercomputers costs many thousands of dollars an hour. By operating many simpler computers, when they were idle for a few minutes or hours, the problem was solved at virtually no cost.

Progress toward factoring a 100-digit number has been rapid this year, even though no new methods of factoring have been developed. Just three weeks ago, the same group led by Dr. Manasse and Dr. Lenstra established another record by factoring a number 96 digits long, and last spring, a Netherlands mathematician, Herman te Riele, factored 92 digits. In the 1980s the record has been broken about once a year, Dr. Lenstra said.

Technique Is Not New

Dr. Andrew M. Odlyzko, a mathematician at A.T.&T. Bell Laboratories in Murray Hill, N.J., said that the basic technique used for the calculation was not new.

The algorithm, or computer method, the team applied, "which is called the 'quadratic sieve,' was invented some years ago by Dr. Carl Pomerance of the University of Georgia at Athens," Dr. Odlyzko said. "In a way, it's slightly disappointing that we have not come up with any real advance over that method in factoring large numbers. There are a lot of variations of the same general method, but they are all roughly equal in efficiency."

The great advantage of the quadratic sieve is that it enables its user to break an enormously complex computational problem down into a large number of relatively simple computations. Each of these computations can be carried out independently and in any sequence.

The strategy, Dr. Lenstra explained, is to calculate a "matrix" of numbers, a square consisting of 50,000 rows and 50,000 columns, in each of which is a number that contributes some information about the solution of the problem. Ideally, a computer could be assigned to calculate each square in the matrix, but in this case, only about 400 computers were available.

"In any case, however," Dr. Manasse said, "we approached the problem as a massively parallel computation, one in which many processors were working

along parallel lines simultaneously. As each small task was completed, the computer user would send us the result by electronic mail.

It Was All There

"Last weekend, we realized that we had enough of these preliminary computations to put them together, using a technique called Gaussian elimination. That gave us the final result last night," he said.

Gaussian elimination is a procedure analogous to the elimination of variables in an algebraic expression by canceling out like values.

Dr. Manasse said that the factoring program had attracted the interest of mathematicians and computer scientists in Canada, West Germany and other countries, and that many had volunteered to participate in a continuation of the program.

Next: 106 Digits

The factoring of a 100-digit number took less than one month, and the pace is likely to continue. "By the end of the winter I would expect that we will have factored a number of 106 digits," Dr. Manasse said.

Asked whether mathematicians had sighted new factoring techniques that might speed the process, he replied: "I'm not anxious to see any radically new techniques emerge. Of course, if they're out there, we'll have to use them. But I would like to see the R.S.A. encryption system continue as a secure safeguard."

All encryption systems are under the continuous scrutiny of the National Security Agency, the federal agency chiefly responsible for safeguarding American ciphers and cracking the ciphers of other nations. Experts from the agency attend meetings of mathematicians and computer scientists and follow academic developments closely.

"It's a safe bet that the N.S.A. knows all about what we've done," Dr. Manasse said, "although we've had no communication from them. In any case, this is not going to give them nightmares. It may just make the code makers a little more cautious. We've done something that once would have been regarded as practically impossible."

THE QUESTION: 9,412,343,607,359,262,946,971,172,136,
294,514,357,528,981,378,983,082,541,347,532,211,942,640,
121,301,590,698,634,089,611,468,911,681

THE ANSWER: 86,759,222,313,428,390,812,218,077,095,
850,708,048,977 \times 108,488,104,853,637,470,612,961,399,
842,972,948,409,834,611,525,790,577,216,753

*(Source: Dr. Andrew M. Odlyzko,
A.T.&T. Bell Laboratories, Murray Hill, N.J.)
October 12, 1988*

Biggest Division a Giant Leap in Math

By GINA KOLATA

In a mathematical feat that seemed impossible a year ago, a group of several hundred researchers using about 1,000 computers has broken a 155-digit number down into three smaller numbers that cannot be further divided.

The number is about 50 digits longer than any that mathematicians have reported being able to break down in the same way, an unusually long leap in this area of mathematics.

The latest finding could be the first serious threat to systems used by banks and other organizations to encode secret data before transmission, cryptography experts said yesterday.

These systems are based on huge numbers that cannot be easily factored, or divided into numbers that cannot be divided further. For example, the factors of 10 are 2 and 5.

First Break in the System

This is the first time that mathematicians have factored a number of the size used in these coding systems, said Dr. Arjen Lenstra, director the project who is at Bellcore Inc., in Morristown, N.J., the research arm of the Bell operating companies.

To break the huge number into three smaller numbers, which are 7, 49 and 99 digits long, the mathematicians had to find a new method because the one used in recent years was not up to the job. If someone had asked him to break up a 155-digit number a year ago, Dr. Lenstra said, "I would have said it was impossible."

Dr. Andrew Odlyzko, a mathematician at the American Telephone and Telegraph Bell Laboratories in Murray Hill, N.J., said: "This is a great achievement. From the standpoint of computational number theory, it represents a breakthrough."

The number itself was famous among mathematicians as a factoring challenge. In October 1988, mathematicians reported the factoring of a 100-digit number. It is a rule of thumb in mathematics that for every 10-digit increase in the size of a number, the amount of computing needed to factor it increases 10 fold. Until now, factoring advances had come in increments of 10 digits or less.

Secrets Are at Stake

But the practical importance of the result, experts said, is what it might mean to cryptography. In 1977, a group of three mathematicians devised a way of making secret codes that involves scrambling messages according to a mathematical formula based on factoring. Now, such codes are used in banking, for secure telephone lines and by the Defense Department.

In this system, a string of letters in the message are replaced a number. That number is multiplied by itself many times, making a bigger number that helps mask the message. Then the big number is divided by a large number whose factors are secret. The remainder of that division—the amount left over—is the coded message. It can only be decoded by a person who knows the secret factors of the large number.

In making these codes, engineers have to strike a delicate balance when they select the numbers used to scramble messages. If they choose a number that is easy to factor, the code can be broken. If they make the number much larger, and much harder to factor, it takes much longer for the calculations used to scramble a message.

For most applications outside the realm of national security, cryptographers have settled on numbers that are about 150 digits long, said Dr. Gus Simmons, a senior fellow at Sandia National Laboratories in Albuquerque, N.M., who advises the Defense Department on how to make coding secure.

Broader Application Seen

Dr. Lenstra, who also led in the breaking of the previous 100-digit number, said: "For the first time, we have gotten into the realm of what is being used in cryptography. It means it is impossible to guarantee security."

Although the number the group factored had a special mathematical structure, Dr. Lenstra and his colleagues say the factoring method can be modified so it would have broad application.

Others are more circumspect. Dr. Simmons said that although he agrees that the method is generally applicable, he is waiting to see whether it can break down other numbers quickly enough to be practical. The method, he said, "may become of concern to cryptographers, but that depends on how efficiently it can be implemented."

Nonetheless, Dr. Simmons said, he would not feel comfortable advising the use of a 150-digit number to maintain security. "If national security were hidden behind a 150-digit number, we're getting very close to a situation where it would be feasible to factor that," he said. "Do I advise the government to use bigger numbers? You bet."

The newly factored number was the largest number on a list mathematicians keep of the 10 Most Wanted Numbers, which are large numbers that are set up as a challenge to factoring experts. And it is so large that it is inconceivable to even think of factoring it without special mathematical tricks.

Answer in a Few Months

Dr. Mark Manasse of the Digital Equipment Corporation's Systems Research Center in Palo Alto, Calif., calculates that if a computer could perform a billion divisions a second, it would take 10 to the 60th years, or 10 with 59 zeros after it, to factor the number simply by trying out every smaller number that might divide into it easily. But with a newly discovered factoring method and with a worldwide collaborative effort, the number was cracked in a few months.

The new factoring method was discovered last year by John Pollard of Reading, England, and Dr. Hendrik Lenstra Jr. of the University of California at Berkeley, the brother of Dr. Arjen Lenstra. The two mathematicians found a shortcut to factoring numbers of a particular form that happened to fit the form of many large numbers that were purposely derived so as to be difficult to factor.

Then Dr. Manasse and Dr. Arjen Lenstra recruited computer scientists and mathematicians from around the world to help in the factoring effort. Each person who agreed to help got programs sent electronically to their computers and a piece of the problem to work on.

Like a Jigsaw Puzzle

It was like solving a giant, and twisted, jigsaw puzzle, Dr. Manasse said. Each computer was set to work doing the mathematical equivalent of sorting through a box with about 50 million pieces "including all sorts of useless stuff that look like jigsaw pieces that are not," Dr. Manasse said, adding: "Each person has to find the real pieces in the box. Some boxes don't have any and some have just one or two."

After about a month, the researchers got back the equivalent of about two and a half million pieces of the puzzle. To speed up the search and the final putting together of the pieces that would allow them to factor the number, the researchers used a powerful computer at the University of Florida that finished the job for them in three hours.

The current factoring landmark is the latest in a series of what to mathematicians have been breathtaking feats. In 1971, mathematicians scored a coup by factoring a 40-digit number. Ten years ago, a 50-digit number was thought to be all but impossible to factor. Then, with advances in research that led to unexpected shortcuts, 60-, 70- and 80-digit numbers fell. A year and a half ago, the 100-digit number was cracked.

June 20, 1990

Scientists Devise Math Tool to Break a Protective Code

By JOHN MARKOFF

Two Israeli scientists have developed a powerful mathematical technique that for the first time makes it possible under certain circumstances to break the code used by many businesses for encrypting highly sensitive information.

The code, which depends on a government system, the Data Encryption Standard, now appears to have a significant chink in its armor, even though experts say it is not immediately threatened by the new mathematical attack.

Information that is often encrypted includes designs for high-tech products, data about oil and other energy reserves and records of financial transactions. Government officials have become increasingly concerned that this material is vulnerable to manipulation or theft as more of it is transmitted between computers.

The encryption standard "is clearly showing its age, and over the next few years we're going to have to figure out something else," said Ronald Rivest, a computer scientist and cryptographic expert at the Massachusetts Institute of Technology.

The two Israeli scientists, Adi Shamir and Eli Biham, have not yet published their results, but Dr. Shamir recently sent electronic mail messages notifying several American colleagues of the breakthrough. The new approach relies on a systematic mapping of subtle variations in very large samples of statistics.

No System Switch Is Seen

Several corporate officials said that the limited breakthrough would not make the Data Encryption Standard obsolete immediately and that switching to other encryption systems would be risky because they had not been extensively verified.

"If I were going to buy cryptographic gear tomorrow I will still buy D.E.S.," said Leslie Chalmers, chairman of the security and risk management division of the American Banking Association. "Using D.E.S. is still preferable to running bare."

Ms. Chalmers said the banking industry chose to rely on government standards because such cryptographic approaches were the most thoroughly tested.

Dr. Shamir, who is a professor of applied mathematics at the Weizman Institute in Israel and one of the world's leading cryptographers, said in a

telephone interview that he did not wish to comment on his work until its publication in a scientific journal later this year.

Although other experts are thus unable to review his work, a number of government and academic scientists said that because of Dr. Shamir's standing in the field they were confident that he was accurately describing his achievement.

News by Computer Message

In a computer message describing his attack on the encryption standard, Dr. Shamir wrote that he was able to "finally break the full 16-round D.E.S." He said his approach was now considerably faster than an earlier method in which a computer tests every possible key to unlock the code. Dr. Biham worked with Dr. Shamir as a student and is now at the Technion, the Israeli research university.

The encryption standard uses a system based on a secret number, or key, that is used to perform a series of mathematical scrambling operations on a message or on other computer data. When the code message is received, the same secret key is used to reverse the process and unscramble the data.

The decoding technique is referred to as a "chosen clear-text attack" in which the cryptographer is assumed to possess the coded text of any message of his choice. Such an approach is realistic only if the code breaker can trick his opponent into encrypting an already known message.

When the known message has been unraveled from its encrypted form by the new method, the original secret key can be derived, enabling the code breaker to solve all messages sent with that key.

Cryptographic research takes place in two separate lines of work. Academic researchers think of themselves as being on the "light side" and insist on openly sharing results. The "dark side" group of cryptographic researchers works behind closed doors at intelligence and military agencies like the National Security Agency. Little is known about their activities or scientific progress.

Original Work at I.B.M.

The Data Encryption Standard is based on research that was originally done by experts at the International Business Machines Corporation's Thomas J. Watson Research Laboratory in the 1970s as part of a project code named "Lucifer" and adopted as a national standard in 1977.

The standard has been a source of controversy because the final version, developed by scientists at the National Institute of Standards and Technology in cooperation with the National Security Agency, shortened the mathematical key used to code and decode information.

Some academic scientists have suggested that the security agency shortened the key to make it possible for organizations like itself, and other American intelligence agencies that have sufficient computing power, to break the code if they really needed to by using brute computer force to try all the possible combinations. This would make breaking codes impossible for anyone but those who have access to multimillion-dollar supercomputers. An exhaustive search to break the code requires 60 quadrillion computations.

The government recertified the D.E.S. in 1988 for commercial and non-classified government use.

An I.B.M. cryptographer said that based on his familiarity with Dr. Shamir's earlier work it was unlikely that the standard was in any immediate danger.

"It depends on the numbers," said Donald Coppersmith, a scientist who participated in the original I.B.M. research. "It still seems to be perfectly adequate for the purposes it was designed for."

Martin Hellman, a cryptographer at Stanford University, said: "There have been questions about the security level of D.E.S. since it was advanced, now we have the final verification that the system can be broken. I would encourage people to buy equipment that can be upgraded in the future."

October 3, 1991

Tied Up in Knots, Cryptographers Test Their Limits

By GINA KOLATA

Edgar Allan Poe thought there was no such thing as an unbreakable code. "It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve," he wrote.

In this spirit, cryptographers have spent nearly 15 years picking at a code that the National Security Agency, the nation's code-making and code-breaking agency, helped design for business and government to use in banking and in transmitting sensitive, but unclassified, data over computer lines. Yet, to the surprise of many mathematicians and computer scientists, the code, known as the Data Encryption Standard, or D.E.S., has stubbornly resisted their efforts to penetrate it. Only recently has anyone found a dent in the code and that dent by no means breaks it. In fact, the new system is only a slight improvement over the laborious method of trying every possible key to the code until the correct one is chanced upon.

The encryption standard is "a Gordian knot," said David Kahn, author of *The Codebreakers* and *Seizing the Enigma*.

Poking away at the code has become an unofficial hobby for many civilian cryptographers, whose frustrations have led them to ask, What is the N.S.A.'s secret in building codes? The N.S.A., whose initials, some say, stand for Never Say Anything, is not commenting, of course.

"N.S.A. sure knows a hell of a lot more than we do," said Dr. Cipher Deavours, the son of a cryptographer who is himself a cryptographer at Kean College in New Jersey and editor of *Cryptologia*, a journal for the field. "Whoever had his finger in designing the D.E.S. sure knew what he was doing," Dr. Deavours said.

Dr. Thomas A. Berson, a communications security expert in Palo Alto, Calif., agreed. "The fact that the D.E.S. has withstood attack from all quarters for so long shows it has amazing strength," he said. In fact, the slightest change in the code makes it easier to crack. "That demonstrates to me that there is theory about making codes that is not known to the outside world," he said.

To mathematicians and computer scientists, the encryption standard is a nagging challenge, a publicly available code that seems to thumb its nose at their attempts to crack it. These researchers believe that by exposing a weakness, they could protect those who rely on the code, warning them that others who

are not so friendly might have discovered for themselves the Achilles heel and may already be reading their mail.

The D.E.S. takes a message, translated into the computer language of zeros and ones, and scrambles it by repeatedly applying mathematical operations. Like a lock with many possible combinations, the code has a family of many possible operations that can be used to scramble a message. Once one of these keys has been chosen, anyone who has it can encode or decode a message. To break the D.E.S., a spy would have to figure out the user's key.

The difficulty is that there are 2 to the 56th possible keys, which is about 72 thousand million million. A computer built especially to break the code could check all the keys in two hours, said Dr. Martin Hellman of Stanford University. But the machine would cost \$10 million. For most people who wanted to decrypt unclassified data, an exhaustive search is likely to be too much trouble and expense. So mathematicians and computer scientists have been looking for shortcuts.

The recent attack on the D.E.S. was announced by Dr. Adi Shamir of the Weizman Institute in Israel, and his former student, Dr. Eli Biham. In a tantalizing message that they sent to friends through electronic mail, they claimed to have found a weakness in the code that makes breaking it slightly easier than trying every combination. The attack is still not practical because it requires nearly as many calculations as an exhaustive search. And it requires an encoded copy of a known message, meaning that a spy would have to somehow plant a message to be encrypted.

Dr. Shamir, in a telephone interview, said he will not reveal the details of his work until it is published in a few months. He said, however, that it is a refinement of a previously published method in which he was able to attack a simplified version of the D.E.S. by comparing unencrypted blocks of text with encrypted blocks and looking for patterns.

Dr. Shamir's reluctance led Whitfield Diffie, a cryptography expert at Sun Microsystems in Mountain View, Calif., to comment, "Adi is a master of the suspense campaign."

Not only did Dr. Shamir not break the D.E.S., but he found, in probing the code, that it is actually far stronger than anyone had imagined. In fact, Dr. Shamir said, it seems to be the strongest possible code of its kind. Dr. Shamir's method devastates similar codes. He and Dr. Biham reported in a previous paper that they can use their methods to crack a competing family of codes that were proposed recently by the Japanese and that were on the verge of being accepted internationally.

Without a Clue

What this means, said Dr. Deavours, is that "we do not have the slightest idea of what distinguishes a good code from a bad one." The Japanese codes, he said, "were claimed to be as secure as the D.E.S. and more appropriate for regular computers," because they did not require a special purpose chip for encoding and decoding. "Imagine the standards organization getting ready to accept this stuff and the next day cracking them turns out to be a footnote in Shamir's paper," he said.

Although reluctant to generalize, Dr. Berson agreed that "there's no theory for developing a cryptosystem." Except, apparently, within the N.S.A.

When they first began working on the D.E.S., mathematicians and computer scientists predicted an easy victory. Some argued that the N.S.A. would never have promulgated a code, to be widely used and sold, that it could not break. If an enemy used the code, the N.S.A. would want to read the enemy's messages. So some civilian cryptographers argued that the code must have a trap door—a secret way of breaking it. Once they found the trap door, they would be in.

Now many doubt that there is such a secret entry. "Not only did no one demonstrate a trap door, but no one has been able to show how you could even make one," Dr. Berson said.

Dr. Shamir agreed. "I would say that, contrary to what some people believe, there is no evidence of tampering with the D.E.S. so that its basic design was weakened."

Asked whether people who use the D.E.S. should be wary, Mr. Diffie said that a lot depends on how and why they use it. In banking, for example, people typically change the key every day. But a message that you hope will be secure for years, even if it falls into enemy hands, might be very vulnerable.

Mr. Diffie said that code breakers have been known to work for decades trying to decipher important messages. For example, in the 1930s, the British intelligence service got hold of an encrypted Soviet message thought to include the identities of spies. "They continued trying to read it for 30 years," Mr. Diffie said.

"If you are designing cryptosystems, you've got to think about long-term applications," he said. "You've got to try to figure out how to build something that is secure against technology in the next century that you cannot even imagine."

October 13, 1991

A Public Battle over Secret Codes

By JOHN MARKOFF

An issue long relegated to testy grumbling between software engineers and intelligence agents has suddenly grown into a public dispute between the Bush administration and business executives.

In a digital age that finds more and more information protected by elaborate coding techniques, both sides are asking: Who should hold the keys to the codes?

Not the government, say members of an increasingly militant computer and software industry. Apple Computer, Microsoft and Sun Microsystems are among the companies vowing to oppose federal efforts to keep tight control on the use of coding technology, known as encryption.

"There is really no way to control this technology," said Nathan P. Myhrvold, vice president for advanced technology at Microsoft. "What are you going to do, call up John Gotti and tell him that it's illegal to use coding technology? All regulations do is hurt people who are trying to be law-abiding, and it's a nightmare for business users who are trying to protect information."

Technique Available to All

Once a tool only of diplomats, military officials and spies, advanced encryption techniques have become available to anyone with access to cheap computer chips.

Nowadays, virtually all information can be translated into digital form and protected with electronic codes—whether it is a cellular telephone conversation, electronic memo, medical record, corporate payroll, television program or cash from the automated teller machine. And advances in hardware and software have made these codes virtually uncrackable to anyone not knowing the precise string of letters or numbers that represents the key to translating the encrypted information.

A House Judiciary panel will hear testimony on the issue today, for the second time in nine days, as Congress ponders whether to resurrect legislation that would give intelligence officials a greater ability to monitor the use of encryption by businesses and individuals.

An alternative move, favored by a growing number of industry executives, would be to scale back government control of computer encryption by

curtailing the powerful National Security Agency's broad jurisdiction over the private use and export of encryption technology. The president has vowed to veto such a bill.

In his concluding remarks at last week's hearing, Representative Jack Brooks, Democrat of Texas, chairman of the subcommittee, indicated that business executives would have a chance in the next session to present their case. "We need to examine closely the claims by industry that the current attempts by U.S. intelligence and law-enforcement agencies to restrict this technology will seriously impair privacy and technological development in our country," he said.

Working on Differences

The computer industry had been trying for months to work out its differences quietly with the N.S.A., the secretive Pentagon branch whose job it is to protect the military's computers and conduct global electronic intelligence gathering. But dissent within the industry and the convening of Congressional hearings have brought the dispute into the open.

Since the first computers appeared in the 1940s, old-line manufacturers like I.B.M. have traditionally cooperated—however grudgingly—with national-security and law-enforcement officials to keep computer codes out of the wrong hands and the keys in the right ones. Such cooperation was wise in the days when the military and the federal government were the largest computer customers. And during the cold war, it was easier for the government to defend its policies.

New Attitude among Companies

But lately, the younger generation of companies that grew up selling business computers, including Apple, Microsoft and Sun, has dug in its heels. The companies argue that government efforts to stifle encryption technology is not only wrong but futile, putting American business at a disadvantage to foreign competitors who face few constraints in creating and using encryption.

"The most important security measures in which any of us engage in our daily business no longer have anything to do with safes, locks guards or badges," said Whitfield Diffie, a computer researcher at Sun Microsystems and one of the nation's leading cryptographers. "Modern security technology has transplanted written signatures and the simple act of recognizing a colleague from the

traditional world of face-to-face meetings and pen-and-ink communications to a world in which digital electronic communications are the norm."

The banking industry is also concerned about the threat of legislation that would force software makers to provide a "trap door," making it easier for federal agents to decipher encrypted files. The industry currently transmits \$350 trillion a year via encrypted wire transfers, and each day United States banks transmit 350,000 encoded messages transferring funds to other nations.

Changing encryption techniques not only would compromise the security of computerized banking transactions but would cost many millions of dollars, said John Byrne, general counsel for the American Banking Association.

But government officials see any costs or inconveniences to business as the trade-off for maintaining law and order. "This is a very real problem," said Kier Boyd, deputy assistant director of technical services of the F.B.I. "Somebody who has a rudimentary knowledge of cryptography can generate something on a personal computer which would give us fits as far as reading it."

The genie, indeed, is out of the bottle. Officials at the Information Technology Association of America, a computer industry trade group, recently obtained a copy of a commercial program called Cryptos written by programmers in Moscow.

Cryptos, which runs on a standard I.B.M. personal computer, encodes data by the two most popular techniques. One is the United States Data Encryption Standard, which the N.S.A. established in 1977 to foster a commercial encryption format that businesses could use (and the government could read, as needed). The second is known simply as R.S.A., an encryption format widely adopted for business use; it was developed outside the N.S.A.'s sphere by academic researchers. The Cryptos package, which is available in software stores in Moscow, sells for about \$200.

The encryption war between American industry and government has been waged on several fronts in recent months. Just last month, for instance, the Justice Department began pressing Congress for a bill that would require telephone companies to install equipment making wiretaps easier to conduct in today's network. The limited introduction of encryption into the telephone network, along with the widespread use of fiber optics and digital transmitters, has made electronic eavesdropping much more difficult than in the days when snoopers needed to do little more than hot-wire a copper phone line.

And it was also last month that some industry executives began charging that the N.S.A. had played a quiet role in limiting the strength of a proposed cryptographic standard for future cellular telephones.

Opposing Needs

"The N.S.A.'s needs run almost directly counter to the economic needs of the country, which include the development of high-technology products based on cryptography," said Marc Rotenberg, national director for the Computer Professionals for Social Responsibility, a public interest group.

Before the International Business Machines Corporation introduced its newest family of mainframes in 1991, I.B.M. tried for more than a year to persuade the N.S.A. to allow it to build a special piece of hardware that would automatically encode information processed by the new computers. Finally, after unsuccessful meetings that went as high as Adm. William O. Studeman, director of the agency at the time, and high-ranking I.B.M. officials, the company threw up its hands. It now submits individual license requests for each export sale—and is frequently turned down.

Corporate executives and industry consultants who have experience in dealing with the N.S.A. say that despite the end of the cold war and the growing importance of cryptography for business purposes, they expect the agency to continue resisting any fundamental challenges to its control.

Still, industry pressure has apparently led the agency to attempt to negotiate a compromise with American software publishers.

The industry had originally backed trade legislation, still pending, which would move control over cryptography exports from the N.S.A. to the Commerce Department. But because the Bush administration has threatened to veto the legislation, the software publishers have quietly attempted to arrange a deal.

But, the largest American computer makers, including I.B.M. and the Digital Equipment Corporation, have refused to participate in the negotiations, saying privately that the weakened R.S.A. would not be acceptable to their customers.

The nominee for the job of director of the N.S.A., Rear Adm. John M. McConnell, declined to be interviewed for this article. Michael S. Conn, chief of information policy for agency, said that national security concerns with cryptography could not be dealt with in a public debate. But the agency, he said, remains confident that it can "continue to meet our mission demands in light of advances in technology."

May 7, 1992

U.S. Code Agency Is Jostling for Civilian Turf

By JOHN MARKOFF

The National Security Agency is trying to establish a standard for electronically scrambling computer communications, a move that would go far beyond the agency's usual military and intelligence domain to include civilian activities like electronic tax returns and computerized medical payments.

The plan by the N.S.A., which may be announced as early as today, worries business executives and privacy advocates, who fear government encroachment. And some officials in the Clinton administration believe that the N.S.A. is overstepping its bounds.

The highly secret federal agency is responsible for electronic surveillance of global communications, though usually not civilian communications, within the United States.

But in an era when everyday business is increasingly conducted over computer networks, and when much of that electronic commerce is transmitted in scrambled form to prevent eavesdropping or theft of information, the agency is intent on having government and civilian computer users employ a standard approach to scrambling.

That way, after obtaining a court's permission, law enforcement officials would have a way of cracking codes.

The National Security Agency will seek bids from companies to produce circuit cards based on its technology, which would be used to scramble electronic messages for government agencies and, eventually, private companies. Agency employees confirmed the plan late Friday, though no agency officials could be reached over the weekend for further details.

I.R.S. Testing Technology

The Internal Revenue Service, the government agency that has the most electronic communication with the public, has already started testing the system. "We need to know what the administrative issues are with this technology," said Henry Philcox, the tax agency's chief information officer.

Many computer industry executives oppose the National Security Agency's

effort, saying there is no way for industry specialists and outsiders to determine the reliability and security of the underlying scrambling technology, which the agency intends to keep secret.

Privacy-rights advocates, meanwhile, are wary of the system because of the electronic "back door" it contains, permitting government eavesdropping. And some other administration officials say that the agency is going too far by pushing the standard into civilian computing.

"What these guys are trying to do is run ahead of the blocking," an administration official who spoke on the condition of anonymity said. "Trying to sell this as the wave of the future is premature as administration policy."

The circuit card, which is designed to fit into a personal computer and which the agency calls Tessera, is based on technology similar to a device known as the Clipper Chip, a telephone voice-scrambling chip that provides a back-door means for letting law enforcement officials eavesdrop.

The Clipper plan, developed by the National Security Agency in cooperation with the National Institute of Standards and Technology, a Commerce Department agency, was announced in April by the Clinton administration. It has been almost universally opposed by computer and telecommunications executives and by public policy groups.

Letter Protests Secrecy

In a letter to be sent to President Clinton today, which was released on Friday to *The New York Times*, a group of 38 of the nation's leading computer scientists, computer-security specialists and privacy experts have urged that the Clipper program be stopped.

"The current proposal was developed in secret by Federal agencies primarily concerned about electronic surveillance, not privacy protection," the letter states. "Critical aspects of the plan remain classified and thus beyond public review."

The letter was signed by most of the civilian pioneers of modern cryptography, including Whitfield Diffie of Sun Microsystems, Ralph C. Merkle of the Xerox Corporation, Martin Hellman of Stanford University and Ronald Rivest of the Massachusetts Institute of Technology.

While there has been no other indication so far that the government wants to force private industry to use Clipper or Tessera technologies, their adoption as government and military standards could go a long way toward making them de

facto standards. The federal and military markets are some of the largest for the computer and communications industries, and the government has the power to determine what sorts of advanced technology can be exported.

Moreover, the government could insure widespread use of the Clipper and Tessera technologies by insisting that they be used by businesses and individuals when communicating electronically with federal agencies.

Official Reasoning

Law enforcement officials say the technologies are intended to resolve a long-standing problem of the information age: how to preserve the right of businesses and citizens to use codes to protect all sorts of digital communications without letting criminals and terrorists conspire beyond the law's reach. Businesses and individuals who often communicate over computer networks already make use of a variety of scrambling systems—either of their own devising or those commercially available.

Many of these scrambling systems are unbreakable by anyone who does not hold the electronic keys to the code, something generally known only by the sender and the recipient of scrambled messages.

That is a problem for the National Security Agency, which routinely listens to many of the world's telephone and computer conversations—although it has no jurisdiction for monitoring non-government conversations within the United States. The N.S.A.'s Tessera and Clipper systems would have an independent agency hold master keys to the codes, which could be obtained with a court's permission for surveillance by law enforcement officials.

Agency Has Wider Vistas

The agency plans initially to purchase 10,000 to 70,000 of the Tessera cards for its use and that of the Pentagon. In an industry briefing held earlier this month, however, N.S.A. officials proposed the eventual use of the secure communications card in a vast range of civilian and government applications including some by the Internal Revenue Service, the Departments of Health and Human Services, Justice and State, and in the Senate and the House.

The agency also suggested that the card could be used for civilian functions like electronic mail and in the scrambling systems employed in cable television.

The National Security Agency's new standard-setting effort is being introduced a couple of weeks before the Clinton administration completes a classified review of the Clipper proposal, and several industry executives said the announcement had been timed to apply pressure to the administration's decision making.

Government-Industry Argument

The proposal angers industry executives who believe that the agency is rushing to establish a de facto standard that will undercut efforts to adopt a competing commercial standard without a built-in back door. That standard, being developed by R.S.A. Data Security, a Redwood City, Calif., software company, has been endorsed by the nation's leading computer makers, software developers and telecommunications companies.

These companies are particularly troubled by the National Security Agency's refusal to disclose the mathematical formula, or algorithm, on which its scrambling technology is based.

"The issue here is: Should a secret algorithm developed by the intelligence community be used for unclassified civilian uses?" said Stephen Walker, a computer security industry executive and a member of the government's Computer System Security and Privacy Advisory Board. "I think the answer is it should not."

The agency has increasingly come into conflict with industry and public policy groups who argue that independent and public coding technology is essential if the nation is to develop a viable electronic commerce system.

"These government surveillance plans focus on limiting public privacy at a time when everyone is calling for more privacy," said Marc Rotenberg, Washington director of Computer Professionals for Social Responsibility, a public interest group that organized the letter that will be sent to President Clinton today. "Privacy is a key part of the national information infrastructure, and the decisions the administration is making are leaning in the wrong direction."

Fragile Job Security

The new security standard is being proposed at a time the National Security Agency is trying to redefine its role after the cold war, and it raises questions in critics' minds about whether the agency is overstepping its authority. The 1988

Computer Security Act limited the N.S.A.'s computer security role to military and intelligence agencies.

"These guys are fighting for job security," said William Ferguson, vice president of Semaphore Inc., a Santa Clara, Calif., computer network security firm. "Now that the K.G.B. has gone commercial, the N.S.A. is trying to start its own initiatives that say, 'all we're trying to do is keep up with the K.G.B.'"

White House officials said the agency's actions would not necessarily force the administration to authorize an unpopular coding technology.

One official said the administration policy review was likely to establish a permanent working group that would limit the National Security Agency's role in policy making.

The agency originally planned to announce its request for proposals on Friday. But the notice was delayed because the government shut down Thursday in response to the frigid weather that disrupted the supply of electricity in Washington and other parts of the East. The agency tentatively plans to award contracts for the Tessera card by March 25.

January 24, 1994

Researchers Demonstrate Computer Code Can Be Broken

By SARA ROBINSON

An international team of researchers demonstrated this week that it was possible to break the security codes commonly used to protect financial transactions over the Internet.

The actual feat involved finding the two prime factors for a number about 155 digits long. The answer enables one to obtain the key used to decode a particular piece of encrypted data.

While the seven-month effort required a significant amount of computing power—involving 292 computers at 11 sites in 6 countries—it showed that the standard level of encryption for Internet transactions, known as 512-bit encryption, was not secure.

"We have said for a long time that 512 is not a secure standard," said Burt Kaliski, chief scientist for R.S.A. Research in San Mateo, Calif., a part of Security Dynamics Technologies' R.S.A. Data Security Inc., which makes encryption technology and sponsored a challenge to break the 512-bit code. "I don't think this means that overnight, Web sites will be attacked, but we need to make the transfer to a larger key size."

The feat also raises questions about the government's policy of export controls on encryption. The 512-bit system has become the standard because, with some exceptions, it is the most secure encryption allowed for export.

Although higher levels of encryption exist, experts estimate that 95 percent of Internet commerce uses the 512-bit standard.

Last September, the administration announced that the export policy would be reviewed and an update announced within one year.

William A. Reinsch, the Under Secretary of Commerce for Export Administration, said today that the administration would make an announcement by mid-September. He could not say, however, what impact the recent demonstration would have on the encryption policy of the United States.

"Our policy is intended to track market developments, but it's too soon to come to a conclusion on this," he said.

Being able to factor a 512-bit number enables one version of what is known as the R.S.A. public key encryption system to be broken. R.S.A., designed in the

mid-1970s by Ronald Rivest, Adi Shamir and Leonard Adleman, is used extensively in software to protect electronic data traffic.

R.S.A. and similar encryption systems are based on the fact that it is immensely difficult and time-consuming for even the most powerful computers to factor large numbers.

Although the factoring task took the researchers seven months, they were using a relatively small amount of computing power, mostly overnight and on weekends.

"I think there is a huge potential to speed this up a lot more," said Arjen Lenstra, a computer scientist at Citigroup, and one of the researchers involved in the project. He said that harnessing the computational power available to government agencies or major corporations could enable such codes to be broken in less than one week.

"Microsoft could do this over a Thanksgiving weekend," he said.

In May, Mr. Shamir, a computer scientist at Weizmann Institute of Science in Rehovoth, Israel, presented a paper describing a device, not yet built, that could break a 512-bit code. But until this week, the feat was only theoretical. Mr. Lenstra and Mr. Shamir are working on a way to use the device to further speed the factoring process.

August 27, 1999

Nick Patterson; A Cold War Cryptologist Takes a Crack at Deciphering DNA's Deep Secrets

By INGFEI CHEN



Thirty years ago, Nick Patterson worked in the secret halls of the Government Communications Headquarters, the code-breaking British agency that unscrambles intercepted messages and encrypts clandestine communications. He applied his brain to "the hardest problems the British had," said Dr. Patterson, a mathematician.

Today, at 59, he is tackling perhaps the toughest code of all—the human genome. Five years ago, Dr. Patterson joined the Broad Institute, a joint research center of Harvard and the Massachusetts Institute of Technology. His dexterity with numbers has already helped

uncover startling information about ancient human origins.

In a study released in May, scientists at the Broad Institute scanned 20 million "letters" of genetic sequence from each of the human, chimpanzee, gorilla and macaque monkey genomes. Based on DNA differences, the researchers speculated that millions of years after an initial evolutionary split between human ancestors and chimp ancestors, the two lineages might have interbred again before diverging for good.

The controversial theory was built on the strength of rigorous statistical and mathematical modeling calculations on computers running complex algorithms. That is where Dr. Patterson contributed, working with the study's leader, David Reich, who is a population geneticist, and others. Their findings were published in *Nature*.

Genomics is a third career for Dr. Patterson, who confesses he used to find biology articles in *Nature* "largely impenetrable." After 20 years in cryptography, he was lured to Wall Street to help build mathematical models for predicting the markets. His professional zigzags have a unifying thread, however:

"I'm a data guy," Dr. Patterson said. "What I know about is how to analyze big, complicated data sets."

In 2000, he pondered who had the most interesting, most complex data sets and decided "it had to be the biology people."

Biologists are awash in DNA code. Last year alone, the Broad Institute sequenced nearly 70 billion bases of DNA, or 23 human genomes' worth. Researchers are mining that trove to learn how humans evolved, which mutations cause cancer, and which genes respond to a given drug. Since biology has become an information science, said Eric S. Lander, a mathematician-turned-geneticist who directs the Broad Institute, "the premium now is on being able to interpret the data." That is why quantitative-minded geeks from mathematics, physics and computer science have flocked to biology.

Scientists who write powerful DNA-sifting algorithms are the engine driving the genomics field, said Edward M. Rubin, a geneticist and director of the federal Joint Genome Institute in Walnut Creek, Calif. Like the Broad, the genome institute is packed with computational people, including "a bunch of astrophysicists who somehow wandered in and never left," said Dr. Rubin, originally a physics major himself. Most have never touched a petri dish.

Dr. Patterson belongs to this new breed of biologist. The shelves of his office in Cambridge, Mass., carry arcane math titles, yet he can converse just as deeply about Buddhism or Thucydides, whose writings he has studied in ancient Greek. He is prone to outbursts of boisterous laughter.

He was born in London in 1947. When he was two his Irish parents learned that he had a congenital bone disease that distorted the left side of his skull; his left eye is blind. He became a child chess prodigy who earned top scores on math exams, and later attended Cambridge, completing a math doctorate in finite group theory. In 1969, he won the Irish chess championship.

In 1972, Dr. Patterson began working at the Government Communications Headquarters, where his research remains classified. He absorbed through his mentors the mathematical philosophy of Alan Turing, the genius whose crew at Bletchley Park—the headquarters' predecessor—broke Germany's encryption codes during World War II. The biggest lesson he learned from Dr. Turing's work, he said, was "an attitude of how you look at data and do statistics."

In particular, Dr. Turing was an innovator in Bayesian statistics, which regard probability as dependent upon one's opinion about the odds of something occurring, and which allows for updating that opinion with new data. In the

1970s, cryptographers at the communications headquarters were harnessing this approach, Dr. Patterson said, even while academics considered flexible Bayesian rules heretical.

In 1980, Dr. Patterson moved with his wife and children to Princeton, N.J., to join the Center for Communications Research, the cryptography branch of the Institute for Defense Analyses, a nonprofit research center financed by the Department of Defense. His work earned him a name in the cryptography circle. "You can probably pick out two or three people who've really stood out, and he's one of them," said Alan Richter, a longtime scientist at the defense institute.

In 1993 Dr. Patterson moved to Renaissance Technologies, a \$200 million hedge fund, at the invitation of its founder, James H. Simons, a mathematician and former cryptographer at the institute. The fund made trades based on a mathematical model. Dr. Patterson knew little about money, but the statistical methods matched those used in code breaking, Dr. Simons said: analyzing a series of data—in this case daily stock price changes—and predicting the next number. Their methods apparently worked. In Dr. Patterson's time with the hedge fund, its assets reached \$4 billion.

By 2000, Dr. Patterson was restless. One day, he ran into Jill P. Mesirov, another former defense institute cryptographer, and mentioned his interest in biology. Dr. Mesirov, then director of computational biology at the Whitehead/M.I.T. Center for Genome Research, which later became the Broad Institute, hired him.

"Really, what we do for a living is to decrypt genomes," Dr. Mesirov said. Cryptographers look at messages encoded as binary strings of zeros and ones, then extract underlying signals they can interpret, Dr. Mesirov said. The job calls for pattern recognition and mathematical modeling to explain the data. The same applies for analyzing DNA sequences, she said.

One common genomic analysis tool—the Hidden Markov Model—was invented for pattern recognition by defense institute code breakers in the 1960s, and Dr. Patterson is an expert in that technique. It can be used to predict the next letter in a sequence of English text garbled over a communications line, or to predict DNA regions that code for genes, and those that do not.

Dr. Patterson said he also has a well-honed instinct about which data is important, after seeing "a lot of surprising stuff that turned out to be complete nonsense." Dr. Lander of the Broad Institute describes him as a great skeptic, with the statistical insight to tell whether a signal is "simply random fluctuation or whether it's a smoking gun."

Making that distinction is one of the great difficulties of interpreting DNA. In studying the human-chimp species split, the genomics researchers strove to rule out possible errors and biases in the data.

Dr. Reich, with Dr. Patterson and Dr. Lander, and two other colleagues, used computer algorithms to compare the primate genomes and count DNA bases that did not match, like the C base in gorillas that had become an A in humans. Because such mutations naturally arise at a set rate, the researchers could estimate how long ago the human and chimp lineages separated from an ancient common ancestor.

A DNA base can mutate more than once, however. To correct for that, Dr. Patterson worked out equations estimating how often it occurred; Dr. Reich revised their computer algorithms accordingly. Two strange patterns emerged. Some human DNA regions trace back to a much older common ancestor of humans and chimps than other regions do, with the ages varying by up to four million years. But on the X chromosome, people and chimps share a far younger common ancestor than on other chromosomes.

After the researchers tested various evolutionary models, the data appeared best explained if the human and chimp lineages split but later began mating again, producing a hybrid that could be a forebear of humans. The final breakup came as late as 5.4 million years ago, the team calculated.

The project was "our hobby," Dr. Reich said of himself and Dr. Patterson. Their main work, in medical genetics, includes devising a shortcut to scan the genome for prostate cancer genes.

Whether studying disease or evolution, Dr. Patterson noted, genomics differs from code breaking in one key respect: no adversary is deliberately masking DNA's meaning. Still, given its complexity, the code of life is the most open-ended of cryptographic challenges, Dr. Patterson said. "It's a very big message."

December 12, 2006

Adding Math to List of Security Threats

By JOHN MARKOFF



One of the world's most prominent cryptographers issued a warning on Friday about a hypothetical incident in which a math error in a widely used computing chip places the security of the global electronic commerce system at risk.

Adi Shamir, a professor at the Weizmann Institute of Science in Israel, circulated a research note about the problem to a small group of colleagues. He wrote that the increasing complexity of modern microprocessor chips is almost certain to lead to undetected errors.

Historically, the risk has been demonstrated in incidents like the discovery of an obscure division bug in Intel's Pentium microprocessor in 1994 and, more recently, in a multiplication bug in Microsoft's Excel spreadsheet program, he wrote.

A subtle math error would make it possible for an attacker to break the protection afforded to some electronic messages by a popular technique known as public key cryptography.

Using this approach, a message can be scrambled using a publicly known number and then unscrambled with a secret, privately held number.

The technology makes it possible for two people who have never met to exchange information securely, and it is the basis for all kinds of electronic transactions.

Mr. Shamir wrote that if an intelligence organization discovered a math error in a widely used chip, then security software on a PC with that chip could be "trivially broken with a single chosen message."

Executing the attack would require only knowledge of the math flaw and the ability to send a "poisoned" encrypted message to a protected computer, he wrote. It would then be possible to compute the value of the secret key used by the targeted system.

With this approach, "millions of PCs can be attacked simultaneously, without having to manipulate the operating environment of each one of them individually," Mr. Shamir wrote.

The research note is significant, cryptographers said, in part because of Mr. Shamir's role in designing the R.S.A. public key algorithm, software that is widely used to protect e-commerce transactions from hackers.

"The remarkable thing about this note is that Adi Shamir is saying that R.S.A. is potentially vulnerable," said Jean-Jacques Quisquater, a professor and cryptographic researcher at the Université Catholique de Louvain in Belgium.

Mr. Shamir is the S in R.S.A.; he, Ronald Rivest and Leonard Adleman developed it in 1977.

Because the exact workings of microprocessor chips are protected by laws governing trade secrets, it is difficult, if not impossible, to verify that they have been correctly designed, Mr. Shamir wrote.

"Even if we assume that Intel had learned its lesson and meticulously verified the correctness of its multipliers," he said, "there are many smaller manufacturers of microprocessors who may be less careful with their design."

The class of problem that Mr. Shamir described has been deeply explored by cryptography experts, said Paul Kocher, who is president of Cryptography Research, a consulting and design firm in San Francisco. However, he added that it illustrated how small flaws could subvert even the strongest security.

An Intel spokesman noted that the flaw was a theoretical one and something that required a lot of contingencies.

"We appreciate these and we look at everything," said George Alfs, an Intel spokesman.

In e-mail correspondence after he sent the note, Mr. Shamir said he had no evidence that anyone is using an attack like the one he described.

November 17, 2007

Prizes Aside, the P-NP Puzzler Has Consequences

By JOHN MARKOFF

The September cover article in *Communications of the Association of Computing Machinery* touched off a distinct buzz last month when more than 10 times the usual number of readers downloaded the article in the first two days it went online.

The subject? A survey of progress being made (not much, apparently) in solving the grand challenge for the fields of theoretical computer science and complexity theory. The problem is described rather opaquely as P vs. NP, and it has to do with real-world tasks like optimizing the layout of transistors on a computer chip or cracking computer codes.

Like earlier grand math challenges like Fermat's Last Theorem, there is a lot at stake, not the least of which is a \$1 million cash prize that was offered for the solution as one of seven Mount Everest-style "Millennium Problems" the Clay Mathematics Institute offered almost a decade ago.

So far no one appears to be close to picking up a check. The challenge, in its simplest, but not most understandable phrasing, is to determine whether or not P equals NP. P stands for the class of problems that can be solved in polynomial time, or reasonably quickly. NP stands for the class of problems that can be verified in polynomial time—quickly. If it can be shown that $P = NP$, then it is possible that the world will be a very different place.

The issues center around a group of classic computer science problems, like the traveling salesman problem—how to figure out the most efficient route through a number of cities given certain constraints. Factoring a large number is also a good example of what is referred to as an NP problem. At present, there is no understood method for doing it in polynomial time, but given an answer it is easy to check to see if it is correct.

The most efficient layout of transistors on a computer chip is another example of problems that are said to be NP.

The allure of the challenge, in addition to the fame and the money, is that if it is possible to prove that P does in fact equal NP, some of the hardest computing challenges may collapse, leading to a burst of new economic and technological productivity.

All of the tasks above, like the traveling salesman problem, are similar in that as the problems grow in size—one more city for the salesman, one more transistor for the chip—the computing time required to solve them increases exponentially. In other words, one more city makes the problem 10 times harder.

Checking to see if any particular solution is correct is simple, but finding the best solution in the case of very large problems is infinitely difficult.

“There are a lot of smart people who have tried to solve this problem and failed,” said Patrick Lincoln, the director of the computer science laboratory at SRI International, a research group based in Menlo Park, Calif. “But they also failed to prove the problem can’t be solved.”

The editors of the journal said they were tickled to have a hit article on their hands.

“I don’t think we’ve ever had an article that started off with this kind of a bang,” said Moshe Y. Vardi, a Rice University computer scientist who is editor in chief of the journal. “Our e-mail blast went out and thousands of people felt they had to click.”

The author of the article, Lance Fortnow, a computer scientist at Northwestern University McCormick School of Engineering, initially told Dr. Vardi that the article would be a short one. “Still open,” he writes, was in first reaction to writing about the state of the work on solving the problem.

There remains a glimmer of hope, he noted. An esoteric branch of mathematics known as algebraic geometry may offer an avenue to prove or disprove the problem, which was first outlined by Stephen A. Cook, a University of Toronto computer scientist, in 1971.

That prospect feels a bit intimidating. As Dr. Vardi said, “It’s a bit scary because we have to start learning a very difficult mathematical field.”

October 7, 2009



CHAPTER 6

Computers Enter the World of Mathematics

AS SOON AS COMPUTERS WERE INVENTED, THEIR POTENTIAL in mathematics was clear. As early as 1927 there was a *Times* article about a “thinking machine” that was sort of a primitive computer. It “requires from eight minutes to a few hours to make computations which would take from a month to a year to work out with ordinary methods.”

Yet as computers became more and more powerful, the questions being asked became more and more intriguing. Of course, brute force calculations were always important, but mathematicians also began asking whether there were some problems that were simply beyond the reach of computers to solve, even if the computers worked until the end of time doing calculations. Some of the problems in question were simple to state. One, called the traveling salesman problem, asks what is the shortest route that connects every one of a cluster of points. That’s easy when there are just a few points. Anyone, or any computer, can just try every route and select the shortest one. But when the number of points grows huge, the number of possible routes that must be checked explodes. Soon it is impossible to use this method.

But then there were a group of problems that seemed just as hard as the traveling salesman problem but had shortcuts that made them feasible. The two classes of problems were named NP—the problems that seemed impossible—and P—all the rest. A fundamental question arose. Does P equal NP? Is there a way to convert the hard problems into easier ones?

In this chapter, which provides a brief history of computers and mathematics as told through articles in the *Times*, the intriguing, philosophical question of P and NP dangles. The story is not over, and the problem has become one of the outstanding unanswered questions in mathematics.

“Thinking Machine” Does Higher Mathematics; Solves Equations That Take Humans Months

Dr. Vannevar Bush, professor of Electric Power Transmission at the Massachusetts Institute of Technology, with the aid of a staff of research workers, including H. L. Hazen, H. R. Stewart, F. G. Kear and F. D. Gage, has perfected a “thinking machine.” It is an electrical apparatus which solves quickly mathematical problems too complex for the human brain.

The machine, called the “product integrator,” according to Professor Bush, opens fields of research hitherto inaccessible. Work on it began several years ago, with the object of meeting the need for a machine which would automatically solve problems of advanced electrical theory rapidly and accurately. A technical description of the instrument is to be published by the Franklin Institute.

“The product integrator,” Dr. Bush said, “might be called an adding machine carried to an extreme in its design. Where workers in the business world are ordinarily satisfied with addition, subtraction, multiplication and division of numbers, the engineer deals with curves and graphs, which represent for him the past, present and future of the things in which he deals.”

The apparatus requires from eight minutes to a few hours to make computations which would take from a month to a year to work out by ordinary methods.

The foundation of the integrator is a watt hour meter. The mathematician takes the equations which he is interested in and plots them on sheets of paper. These sheets are passed under pointers and operators along the machine keep the pointers along the curves. As the pointers move, the power flowing through the meter varies in proportion.

The meter controls a motor which drives a pencil on another sheet of paper, tracing a curve, which is called the integral and which is the result sought. A second device, somewhat different from the first, but performing the same operation, integrates the result a second time.

Dr. Bush said the apparatus will solve practically any “second order differential equation,” a type with which engineers have often to deal.

Dr. Bush, who is 27 years old and was graduated from Tufts College in 1913, was a specialist on submarine detection devices for the navy during the World War.

October 21, 1927

New Giant "Brain" Does Wizard Work

New mathematical laboratories in which giant "electronic brains" will find speedy answers to complex problems raised in atomic research and aviation have been established by the National Bureau of Standards, it was disclosed tonight.

Dr. Edward U. Condon, director of the bureau, announced the creation of the "National Applied Mathematics Laboratories," which will have branches in New York, Los Angeles and Washington.

Two ultra-high speed electronic computing machines, said to be faster and better than any previous device, already are being built for the new laboratories.

Dr. Condon revealed that the new machines, to cost about \$300,000 each, would be capable of solving in ten minutes a problem which a skilled mathematician working day and night by ordinary means would require three years to complete.

Bureau of Standards officials believe the new machines will save both time and money in vital scientific research.

For example, one of the basic problems in aircraft design concerns the amount of "flutter" a wing structure will show under certain strains. At present, costly wind tunnels and other direct experiments are necessary, sometimes at grave risk to pilots' lives.

Result of War Developments

To solve the problems mathematically would require about 5,000 hours of computation on the most efficient machines now available. The new machines could solve such problems in one hour, the bureau said.

Dr. Condon indicated that the electronic brains were not a new invention, but an improvement in the pioneering developments of the war.

"Forefathers" of the new brains include:

1. The "electro-mechanical" calculator built at Harvard by the International Business Machines Company.
2. The "relay-type" computing machines developed by Bell Telephone Laboratories.

3. The famed "ENIAC" at the University of Pennsylvania, first purely electronic computing device, developed by two scientists connected with the university, who were subsequently employed by the Electronic Control Company.

Private industry, including the Electronic Control Company and the Raytheon Corporation, was cooperating in the construction of the new machines, Dr. Condon said.

The Los Angeles branch, called the "Institute of Numerical Analysis," will be established at the University of California. Dr. Condon said it would not only conduct basic research in applied mathematics, but also would act as a "service group" for Western industries, research institutions and government agencies.

The New York branch will be designed the "Mathematical Computation Laboratories." It is an outgrowth of a wartime project which rendered invaluable mathematical assistance to industry and the Navy.

Census Bureau May Get Machine

It was indicated that a third computing machine might be built in the near future to speed up the calculations of the Census Bureau.

At present the solution of a typical census problem, involving 100,000 digit numbers, takes about twelve working days. The new machines could do it in 10 minutes, it was stated.

Bureau of Standards experts say the machines under construction will have a "built-in intelligence" which will enable them to handle the most complicated differential equations of physics and engineering, performing hundreds of separate mathematical operations without the intervention of a human operator.

The devices will also have "internal memories" which can store 5,000 or more numbers of twelve digits each, ready for use at the proper moment in the computation. They will handle ordinary computations, such as multiplication or division, in a matter of "micro-seconds"—or about 1/200,000th of the time a human being requires to snatch his hand from a hot stove.

August 25, 1947

"Brain" Speeded Up for War Problems

By WILL LISSNER

ENIAC, the only electronic computer among the four "mathematical brains" now in use, is being converted so that it can handle without resetting all types of mathematical problems to which it is adapted, it was disclosed at the Aberdeen Proving Ground today.

Seventeen percent of the machine time is now lost in changing the set-up by resetting switches and pulling plugs every time the type of problem fed into the robot is changed, Dr. Franz L. Alt of the Ballistic Research Laboratories reported. The loss is higher as the variety of problems is increased.

Col. Leslie E. Simon, director of the laboratories, said the latest change-over was begun five months ago, on the basis of a new mathematical approach by Dr. John von Neumann for the Institute of Advanced Study, Princeton, N.J., and was scheduled to be completed by Christmas. It involves adding a panel of circuits and making other minor structural changes in the machine. These retain the basic design and permit the machine to be reconverted at any time to the former set-up, which gives faster results in computing firing tables and other ballistic work used in wartime research.

Better Machine on Way

The reconversion will give the ENIAC a substantial part of the efficiency which is being built into the Edvac, a more advanced type of automatic computer, employing both electronic and electrical relay circuits. Edvac will not be completed for at least seven months, Colonel Simon said.

Greater efficiency was needed in electronic computing and this could not wait on the completion of Edvac because there was a backlog of six months of top-priority computation in basic research for pilotless aircraft, guided missiles and supersonic flight, the colonel explained. ENIAC is a year or more behind on important but less urgent business, he said.

Dr. Alt said the top-priority work scheduled for ENIAC for the next six months could be done by human computers only in 250,000-man hours.

As an illustration of the type of work being done on ENIAC, Colonel Simon cited the measurement of the path of the V-2 rockets which are being fired at the

White Sands proving range in New Mexico. Nine methods of measurement are employed, including advanced-instrument techniques such as radio and radar, to track the missiles every 2.6 feet they move. Plotting the path requires solving for 900 points and it cannot be done by human computation in time to be of any value. ENIAC does the job in seven minutes.

"Orders" to Robot Reduced

Dr. von Neumann explained that the problem of the conversion involved finding a set-up of the robot's two sets of twenty accumulator tubes which would work for all types of problems.

By an approach through mathematical logic it was found, he said, that the robot could be taught, in effect, a simplified dictionary instead of directing its operation by 350 to 380 orders having a highly complex inter-relationship. It was found that the orders could be reduced to sixty from seventy. That could be put on punch cards and checked by a machine developed by the International Business Machines Corporation. This approach requires the mathematician to translate his problem into sixty orders.

One advantage, Dr. von Neumann said, is that the new system of operation more nearly approximates the operation of the human brain in mathematical thinking and avoids errors in preparing problems for the machine. It requires more human brains in the form of mathematicians, however, for the preparatory work. Although the machine is still operated by magnetic tape, the problem is fed into the machine from punch cards and the solution is printed on punch cards.

The new coding technique is being demonstrated to 300 members of the Eastern Association for Computing Machines who are attending a meeting that closes tomorrow morning.

December 13, 1947

The Electronic Digital Computer: How It Started, How It Works and What It Does

By HENRY L. LIEBERMAN AND DR. LOUIS ROBINSON

Lord Byron had a flair for poetry and for life but Lady Byron (the “Princess of Parallelograms”) and their only child—Ada Augusta, Countess of Lovelace—appear to have been more intrigued by mathematics. In fact, Lady Lovelace (1815–52) blazed a trail of her own in the arts of computer analysis and programming.

She was fascinated by the mathematician Charles Babbage, visited him frequently and listened avidly as he explained his plan for an automatic mathematical machine called the Analytical Engine. And she left behind, in detailed notes appended to her translation of an article in French on Babbage’s plan, a brilliant description of a machine that “weaves algebraic patterns just as the Jacquard-loom weaves flowers and leaves.”

This mathematical machine of counting wheels, gears and cranks was never completed despite fund-raising schemes such as an abortive plan by Babbage and Lady Lovelace to develop a surefire system for betting on the horses. But what was once called “Babbage’s Folly” turned out to be a really smashing idea.

Babbage (1792–1871), who grew grumpy with age and disappointment, was a mathematics professor at Cambridge in the 1830s. He had a piercing and restless mind, a biting tongue, a visceral distaste for organ grinders, an “inveterate habit of contriving tools” and side interests in such matters as actuarial tables, economic systems analysis, the pulse beats of animals and colored lights for the ballet.

This many-splendored genius built a model of a small Difference Engine that evaluated polynomials by the method of taking differences among numbers. He was involved in a project—never finished—to build a bigger Difference Engine when he conceived the grand design for an even more elegant counting-wheel machine, the Analytical Engine.

It was to have a “store” to hold information to be processed, a “mill” to work on the data and a “control” to provide automatic operation. The control was to be the kind of punch cards introduced in 1801 by the French inventor Joseph Marie Jacquard for automatic loom weaving.

Machine calculation is at least as old as the abacus, but the history of modern calculators dates to the 17th century, when Napier, Pascal and Leibniz all built computing devices. Pascal's calculator is particularly important as the prototype of mechanical calculators now being used.

It remained for Babbage to advance concepts immediately recognizable as having a direct relationship to the way present day digital computers operate. In Babbage's time, however, the technology for carrying out his ideas simply did not exist.

More than a hundred years elapsed before the first machine resembling the Analytical Engine was built. This mechanical computer, conceived by Howard H. Aiken of Harvard, was completed with the collaboration of the International Business Machines Corporation in 1944.

Two years later came the first electronic digital computer—ENIAC (Electronic Numerical Integrator and Calculator)—designed by J. Presper Eckert and John Mauchly of the University of Pennsylvania.

Many men have played pivotal roles in the evolution of technologies important to computer science. Among them are the following:

George Boole (1815–1864), a British mathematician who developed the concepts of symbolic logic.

Norbert Wiener (1894–1964), of the Massachusetts Institute of Technology, whose Cybernetics systematized concepts of control and communications.

Alan M. Turing (1912–54), a British mathematician who formulated a definition of automatic machines, worked out a mathematical model of an elementary “universal computer” and proved theoretically that it could be programmed to do any calculation that could be done by any automatic machine.

John von Neumann (1903–57), a Hungarian mathematician who came to the United States where he developed the concept of the stored program for digital computers.

Claude E. Shannon, now aged 50, of M.I.T., who defined the application of symbolic logic to electrical switching and is even better known for his basic work in information theory.

The stored-program concept involves the storage of both commands and data in a dynamic memory system in which the commands as well as the data

can be processed arithmetically. This gives the digital computer a high degree of flexibility that makes it distinct from Babbage's image of the Analytical Engine.

Babbage's machine program was based on instructions punched into sets of cards. He even conceived of a method of conditional transfer. In such a transfer, a designated result of a calculation, but one unknown in advance, would—in turning out to be, say, a negative instead of a positive number—cause the machine to select an alternate set of cards for a different preplanned set of actions.

Profound Impact

Modern punch cards are often used to feed instructions to the present-day computer. This machine also handles conditional operations as part of its control capabilities. But no card-changing is required. As the computer automatically checks off the instructions to it in sequence, it can modify the commands as well as the substantive contents stored in its memory.

This is possible because both the commands and the data are represented by numbers, and the computer can manipulate numbers generally. For example, if three numbers—16, 1 and 17—are all stored in the memory, with 16 calling for one set of actions and 17 for another set of actions, the computer can shift from one set to the other whenever it is told to add a 1 to the 16.

During the last two decades the digital computer has become a primary element in the great ferment of interrelated change that is transforming the world in which we live and the way we live it. Scientific and technological advances, marked by intensified research and a narrowing of the time between discovery and application, are having a profound impact on the works of man.

The computer has not only been an important tool in the research, but it also has been used as a workhorse device in processing large floods of data produced by an expanding and more intricate economy. Furthermore, the computer has been integrated more and more into the dynamic operational aspects of the economy and its various institutions.

In business, for example, the computer has become an essential tool in management planning and control activities. There is a continuous requirement for improved techniques as well as more efficient methods to deal with the growing amounts of paperwork demanded by a society that is increasingly preoccupied

with reports, analyses, records and detailed documentation.

Aside from its applications in science, industry and business, the electronic digital computer is now being widely used in government, in medicine, in education, in transportation and communications, in the arts—and the list of its specific uses is growing steadily. What is this modern electronic Analytic Engine? How does it work?

Coded Information

Whether it is solving a differential equation on the motion of charged particles or keeping track of a nuts-and-bolts inventory, the digital computer functions as a numerical transformer of coded information. It takes sets of numbers, processes them as directed and provides another number or set of numbers as a result.

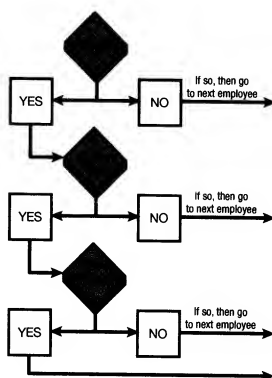
A modern digital computer is composed of elements that provide five essential functional capabilities: input, memory, arithmetic-logic, control and output. An ordinary machine also has some of these capabilities. But the computer is very different.

Among the characteristics that make it different are the flexibility with which it can be adapted generally to logical operations, the blinding speed with which it can execute instructions that are stored within its memory, and its built-in capacity to carry out these instructions in sequence automatically and to alter them according to a prescribed plan.

Despite its size and complexity, a computer achieves its results by doing a relatively few basic things. It can add two numbers, multiply them, subtract one from the other or divide one by the other. It can also move or rearrange numbers, and among other things, compare two values and then take some determined action in accordance with what it finds.

These computer talents, bestowed by man, provide a means of solving multiple problems that can be broken down by man in terms of the factor, "if so, then..." As an example, take the case of a company that must send one of its employees to France quickly. The personnel director is asked to supply the names of candidates who are single, under 35 and able to speak French.

A logical flow chart could be worked out for this set of conditions and personnel cards fed into a computer for sorting-out on the basis of the conditions. The flow chart would look like this:



Elementary as the above procedure is, the same type of logical approach is used in getting a computer to perform a wide variety of calculations, including, for example, Social Security deductions in the processing of payrolls.

Aside from its affinity for logic, the computer obeys with amazing speed. Extra-fast computers can now execute about 10 million steps a second. By way of imperfect but still impressive comparison, each of the myriad neurons of the nervous system handles about 200 switching operations a second.

For all its transistor chips, magnetic cores, printed circuits, wires, lights and buttons, the computer must be told what to do and how. Once a properly functioning modern computer gets its instructions in the form of a properly detailed "program," it controls itself automatically so that it responds accurately and at the right time in the step-by-step sequence required to solve a given problem.

It makes decisions by command and not, as humans often do, by instinct. If the data put into the machine are wrong, the machine will give the wrong answer.

Computer operation begins with the "software," that is, the detailed program needed to instruct the machine.

Developing the software is a very expensive enterprise and frequently more troublesome than designing the actual "hardware"—the computer itself. As an illustration of what the software may involve, it is often necessary to specify 60,000 instructions or more for a large centralized inventory-control system.

Software development calls for a thorough analysis and systematic dissection of a given problem, the preparation of the kind of flow-chart plan shown above to conform with the machine's capacities and the translation of the required steps into a language that the machine understands. It also involves, finally, the debugging of the program to test its correctness in a wide variety of situations.

For an understanding of what is required of a machine to solve a problem, consider the matter of controlling the quantitative level of a particular set of items in a manufacturer's inventory.

Inventory control is a complex and varied procedure, but the key questions can be formulated into mathematical equations. One such equation, cited here merely as an example, is

$$\frac{S + Q - B}{R} - P + T = D$$

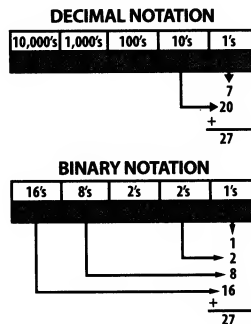
where S = current stock, Q = new stock already ordered, B = stock available but already committed, R = average daily use, P = protective stock or minimum level (expressed in days), T = current calendar day and D = day when new stock must arrive to prevent a shortage from developing.

All the letters above represent variables for which numerical quantities are substituted to describe an inventory situation as it actually exists. Some means must be available, then, to get these numerical quantities into the computer.

This requires an input facility that converts any symbols used outside the machine (numerical, alphabetical or otherwise) into the proper internal code used by the machine to represent those symbols. Generally, the internal machine code is based on the two numerical elements 0 and 1.

In the decimal-number system, each symbol from 0 through 9 is called a digit. As we move one place from right to left in this system, we are multiplying by a factor of 10. In the 0 and 1 system—described as binary—each symbol—0 or 1—is called a “bit,” which is a contraction of the words “binary” and “digit.” As we move one place from right to left in this system, we are multiplying by a factor of 2.

A comparison of binary and decimal notation for the number 27 follows.



The 0s and 1s of binary notation represent the information processed by the computer, but they do not appear to the machine in that form. They are embodied in the ups and downs of electrical pulses and the settings of electronic switches inside the machine.

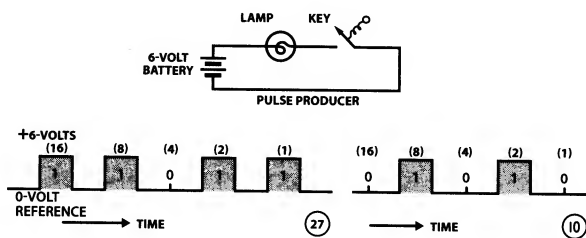
For an understanding of pulse-formation and pulse sequences, it may be helpful to consider an elementary circuit consisting of a battery (say, a 6-volt type), a light bulb and a spring-loaded hand key, all connected, with the operator alternately pressing down on the key and releasing it.

When the key is down, the battery voltage turns on the light with a 6-volt pulse. When the key is released, the lamp voltage becomes 0 and the light goes off. When the key is pressed again, there is another 6-volt pulse and the lamp lights again.

If the hand on the key were steady and the sequence rhythmical, the pulses would occur regularly and be distributed evenly along an imaginary base line whose length represented time. The width of the space occupied by each pulse would depend on the beat, or frequency.

Since the pulses given off by our pulse-producer are either 6 volts or 0, we could call the 6-volt level of each pulse a 1 and the level at which there is no voltage a 0. In effect, then, we can use pulses as the conveyers of binary-coded information.

Our pulse-producing “machine” and pulse sequences for the numbers 27 and 10 in binary code are shown below.



Such pulses can be used to code decimal numbers, alphabetic letters, words, punctuation marks or designs arranged in machine-readable patterns. But more sophisticated means than a simple hand key are used for the computer's input facility. Some advanced inputs involve the scanning of a printed page, the conversion of a limited vocabulary of spoken words and the use of "light pens" to detect information on a television-like cathode-ray tube.

So far as our inventory equation is concerned, the information pertaining to it may be inserted in the computer by any of a variety of input devices. One possible input device is actually a key-driven machine—a typewriter whose keys are connected to electronic networks that convert information into pulse sequences corresponding to notations on the pressed keys.

Such terminal devices may be operated at remote points.

Other input means are provided by punched cards and punched tape, with metal brushes or photoelectric cells sensing the holes and closing an electric circuit each time a hole is sensed. Use is also made of magnetic tape, disks, drums and ink, with the information being represented by different patterns on magnetized spots.

Look at one of your bank checks. The chances are you will find some numerals at the bottom. They are printed with magnetic ink for purposes of data processing.

But getting back to the inventory problem. Once the information pertaining to it is fed into the machine, the data must be lodged somewhere and preserved so that they do not disappear. For example, when a computer is “told” how many inventory items are on hand, it must “remember” that fact—and all other facts associated with the problem.

Storing such information is the function of the computer “memory.”

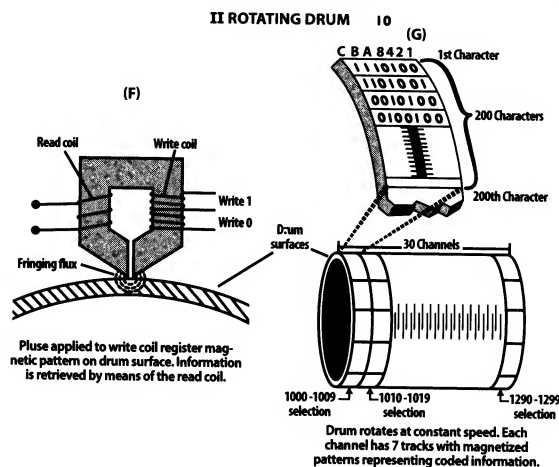
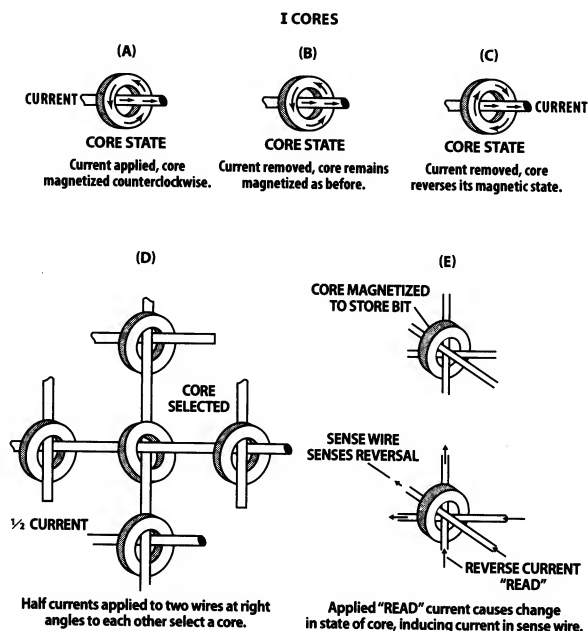
Small packages consisting of ferromagnetic cores are widely used as the computer’s main memory. Magnetic tape, disks and rotating drums are used as auxiliary memories. On such auxiliary devices, information is recorded and retrieved from their surface by “read-write” heads similar to those used for the recording and playback functions on an ordinary tape recorder.

A core, whose dimensions are measured in thousandths of an inch, is a tiny doughnut-shaped object pressed from a mixture of ferric oxide powder and other materials and then baked in an oven.

Millions of cores are used for very large computer memories. They are strung, or “sewn,” into a wire mesh. Then other wires are passed through them into three planes so that appropriate pulses can cause each core to absorb (“read”) or release (“write”) information bits.

In the two sets of diagrams on the following page, I illustrate the principles involved in the use of cores and II the principle of the rotating drums as memory devices.

As shown at (A) of the core illustrations, electric current is sent through the wires to magnetize a core. The core’s magnetic direction, counterclockwise in this



case, is determined by the direction of the current. Even if the current is removed, as at (B), the core remains magnetized in the same direction.

It stays magnetized in this way until the reversal of the applied current causes it change state, as at (C). The two states can be used to represent 0 or 1, plus or minus, yes or no, on or off.

With so many cores strung together, how is a particular core selected for storing a bit? A method of doing so is shown at (D). Two wires run through each core at right angles to each other. Only half the current required to magnetize a core is sent through each wire.

Consequently, only that core receiving full magnetization current from the two wires is selected.

When a core is required to release information, a "read" current is applied to it. This causes a change in state, and the change induces a pulse in the sense wire that amounts to a message from the memory to another part of the computer, as shown at (E).

In the diagrams relating to rotating drums (II), the read-write heads contain coils of fine wire wound around tiny magnetic elements, as shown at (F). A 30-channel drum used for storage in a data-processing system with seven information tracks for each channel is shown at (G).

Means have now been described for getting information into the computer and storing it. Since problems like inventory control are based on equations, however, the computer must at least have the arithmetic capability of adding, subtracting, multiplying and dividing.

In manipulating numerical data inside the computer, it is necessary to shift bits of information or hold them while parts of the machine analyze the data. Sometimes it is also necessary to compare two numbers to see if they are equal, or to see if one is larger than the other, or if the number is 0, and so on.

Indeed, many modern computers provide more than a hundred capabilities such as these, each one of which is built into the hardware.

The computational requirements are handled by the computer's arithmetic-logic unit. Its physical parts include various registers, comparators, adders, complementers and other "logic circuits."

A register is a device that receives information, holds it—usually temporarily—and then releases it as directed by the step-by-step instructions programmed into the computer. Magnetic cores or "flip-flops" are frequently used to form a register.

A flip-flop is an electronic switch. It usually consists of two transistors arranged so that incoming pulses cause them to switch states alternately. One flips on when the other flops off, with the latter releasing a pulse in the process. Thus, multiple flip-flops can be connected to form a register in which binary counting is accomplished by means of pulse triggers.

Stable two-state electronic devices, like the flip-flop, are admirably suited for

processing the 0 and 1 elements of the binary-number system. This, in fact, helps to explain why the binary-number system is commonly used in computers.

Like decimal numbers, binary numbers obey all the rules of arithmetic and can therefore be added, subtracted, multiplied, and divided. Addition is the primary arithmetic process carried out in the computer's arithmetic-logic unit.

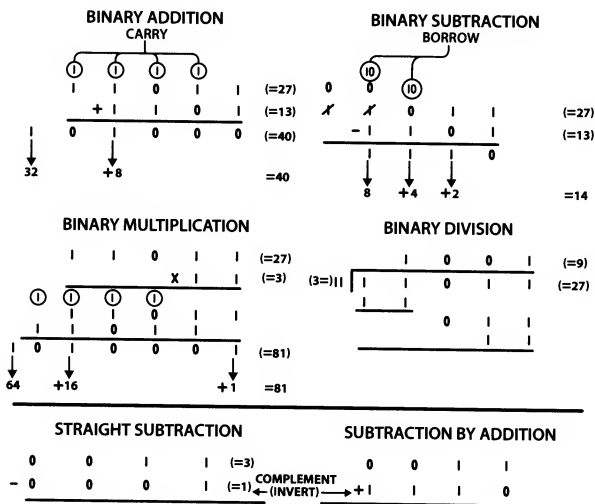
All other operations can be carried out either by addition or variants of addition.

For example, multiplication can be done by repeated addition. Subtraction can be accomplished by complementing one number, adding it to another and then adding an extra 1. And division can be achieved by repeating subtraction.

In the decimal system, the complement of a number can be obtained by subtracting that number from a series of 9s and adding 1 to the result. The complement of 88, for example, is 12.

In the binary system, the complement of a number is obtained by subtracting that number from a series of 1s and then adding the extra 1. This, however, is equivalent to changing all 0s to 1s and all 1s to 0s and then adding 1.

Consequently, in a computer, it is easy to provide simple circuitry to complement a number by inverting it and, in this way, carry out subtraction by means of addition. Basic operations in the binary system, similar to those carried out in the decimal system, and an example of the binary complement are illustrated below:



Logical operations in the computer's arithmetic unit, as well as in other units of the machine, can be represented in an algebra of logic named after the 19th century English mathematician George Boole.

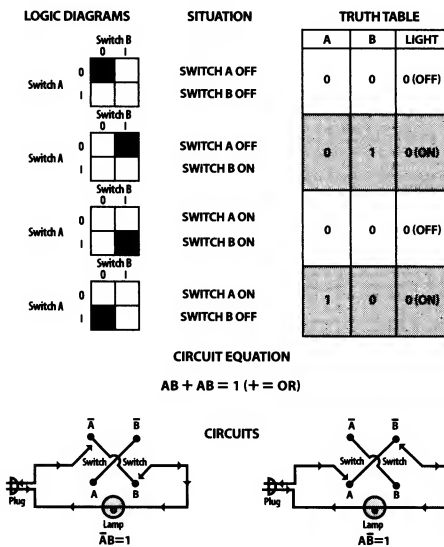
In Boolean representation, the multiplication sign (\times) means AND while the plus sign ($+$) means OR. A bar over any symbol means NOT. An affirmative statement like A can therefore be expressed negatively as $\neg A$ (NOT A).

If a switch is regarded as being in state A when it is closed, then it is in a state of $\neg A$ (NOT A) when it is open. If another switch is connected in series with the first switch and its two states are similarly considered to be B for closed and $\neg B$ (NOT B) for open, then we must have both an A and B for the entire circuit to be completed.

When the A and B conditions are met, the result may be called "true" or "t." Thus, for the two switches in series, the completed circuit may be described by the simple Boolean equation: $A \times B$ (or alternatively, AB) = 1 (the " \times " meaning AND).

Use of the Boolean notation may be illustrated in the design of the familiar upstairs-downstairs light arrangement in which a hall lamp can be turned on or off from either location. The four conditions implicit in the problem may be represented in logic diagrams or, even more effectively, in a "truth table."

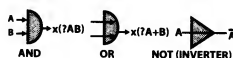
These are shown below with the Boolean equation for the problem and the schematics of the hall-lamp circuitry:



In handling the logic required to process a problem like inventory control, the computer is obviously dealing with more complicated matters than the hall-lamp arrangement. But the logic used in mapping the circuitry for the computer's arithmetic unit is similar, particularly with regard to the important internal connectors known as "gates."

A gate is a logic element that produces an output signal only when a specific set of conditions is met. If the conditions are met, the gate will pass information pulses; if not, it will block the flow. There are three basic types of gates: the OR, which passes data when the appropriate signal is present at any of its inputs; the AND, which passes data only when the same appropriate signals are present at all inputs; and the NOT, which turns a 1-signal into a 0-signal, and vice versa.

Gates are standard package elements in computers. Instead of drawing such circuits repeatedly, computer designers rely on symbols to depict them. Symbols used for AND, OR and NOT gates follow:



The utility of such symbols is demonstrated below for two kinds of computer activity: the transfer of an information bit from one register to another and the addition of two numbers by a half-adder. The half-adder is called that because it can deal only with two numbers to be added and not with a "carry" from a previous stage.

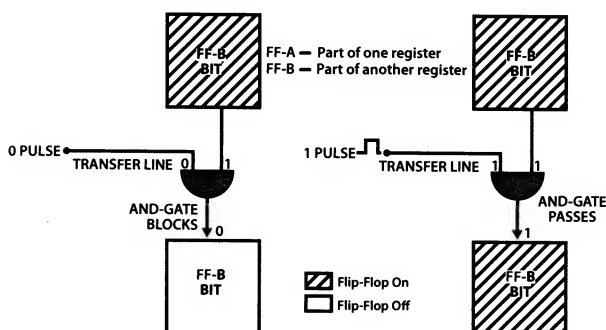
For the data bit to be transferred from FF-A (Flip-Flop A) to FF-B to the right, there must be two appropriate signals of the same kind at the two inputs of the AND-gate. One such signal (a 1 in this case) is already provided by the condition of the FF-A. But the second signal is not present until a 1-pulse is applied over the transfer line.

When the second signal appears over the line in the form of a 1-pulse, the two inputs of the AND-gate are both properly primed and the bit stored in FF-A is duplicated in FF-B. Thus, in effect, the bit has been transferred.

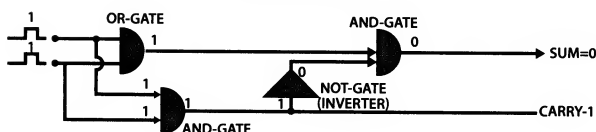
In the half-adder shown, notice that the addition of 1 and 1 in binary arithmetic must produce a sum of 0 and a carry of 1. The circuit accomplishes this. Incidentally, two half-adders can be combined to form a full adder capable of handling a carry from a previous stage as well as two new numbers to be added.

Arithmetic units can be operated serially, with one pulse following the other in a single-file sequence, or in parallel, with the pulses stacked one over the other.

HOW BIT IS TRANSFERRED BY AND-GATE



A HALF ADDER



Parallel operation is the faster method because more can be made to happen in a given time interval.

We have already discussed three facilities basic to the processing of our inventory data—input, storage and arithmetic-logic. But we still have not processed the data. Nor, for that matter, have we established the traffic pattern needed to avert chaos in the computer.

As indicated earlier, the machine must operate in a step-by-step fashion. Thus, it must be told when to add (or subtract, etc.), when to transfer information from the memory to the arithmetic unit, when to store it back into memory, where to look for the next instruction, and so on.

Supervision of these functions is the work of the control unit, the computer's built-in traffic cop. It regulates the internal operations of each unit and the relations between them by means of electrical timing pulses that open and shut connecting gates in the required sequence.

All operations in the computer take place in fixed time intervals measured by sections of a continuous train of pulses. These basic pulses are sometimes provided by timing marks on a rotating drum, but more frequently they are generated by a free-running electronic oscillator called the "clock."

The clock-beat sets the fundamental machine rhythm and synchronizes the auxiliary generators inside the computer. In a way, the clock is like a spinning

wheel of fortune to which has been affixed a tab that touches an outer ring of tabs in sequence as the wheel revolves. If a signal is present at an outer tab when the wheel tab gets there, the appropriate gate is opened.

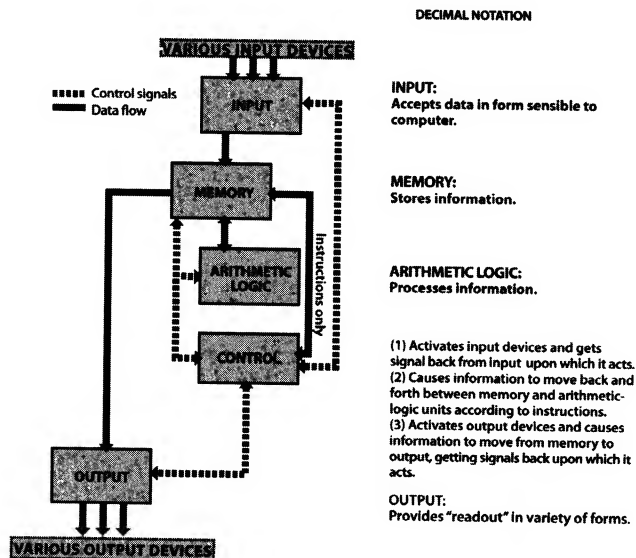
Each time-interval represents a cycle during which the computer carries out part of its duties. One machine operation can be set up for the computer during an instruction cycle (I-time), for example, and then proceed during an execution cycle (E-time).

Now that the control unit has been "added," we have a machine to process information and problems like inventory control. But we still have to get the results out of the computer. The results, stored in the memory after processing, are extracted in the form of pulses and emerge as output "readouts" on devices that look similar to the input devices mentioned earlier.

Among the output systems used are punched cards, magnetic tape, magnetic disks and paper tape. The great demand, however, is for a printed readout. Thus, a great variety of printers is being used for the output requirement.

A recent surge of application development has created a need for other output forms, including graphic displays on cathode-ray tubes, signals for many kinds of control devices and even voice reproduction.

We are now in a position to draw a block diagram of the major computer unit and their relationship to each other:



The block diagram illustrates the functional organization, but not the actual arrangement, of the hardware inside the computer. Control elements, for example, are scattered throughout the machine.

All parts making up the computer, however, are interconnected by wires, printed circuits and gates through which pulse information flows as directed by instructions given to the computer.

These instructions, or program, determine the circuits that will be called upon to solve the problem, the interactions between them and the sequence in which the various machine elements will be called into play.

All modern digital computers can be used to help program themselves. But man is the ultimate controller. The computer stands mute until the instructions that man has written are fed into the machine and the right buttons pressed.

Happily, the programmer—or the computer operator for that matter—does not have to know all about the electronic circuitry inside the computer. On the other hand, the programmer must know the organization of the machine, the kind of statements he can use in communicating with it and how to write these statements sequentially to get the computer to solve the problem he wants solved.

The language used to communicate with the computer is called the “source language.”

Each source language has its vocabulary, its syntax and its repertoire of permissible instructions. An asterisk (*) may mean multiply, a “verb” (operation command) may have to precede a “noun” (data location) and parentheses may have to be related to symbols in specific ways to achieve desired results.

Use of Source Languages

Source languages are usually designated by acronyms. Among those in wide use are ALGOL (Algorithmic Language), COBOL (Common Business Oriented Language) and FORTRAN (Formula Translator). A statement in these languages is much less formidable than it would be if it were written directly in the code used by the computer hardware.

For example, the instruction $\text{DISTANCE} = \text{RATE} * \text{TIME}$ means simply: make distance equal rate multiplied by time.

Obviously, before a computer can deal with such an instruction, there must be some way to convert the source-language statement into the appropriate series of machine-language instructions. The translation is accomplished by a computer

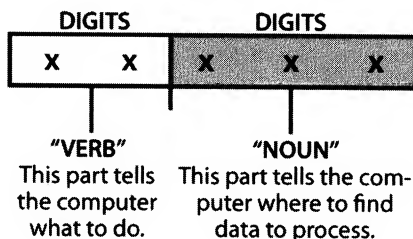
program (set of instructions) previously written and stored in the machine's memory.

This type of program is called a "compiler." A given source language is associated with a particular compiler.

The memory may be regarded as consisting of a vast set of "mailbox"-type slots. Each slot has a designation number called an "address" and each is large enough to hold a stipulated number of digits. (We will be dealing below with decimal digits, which are, in fact, the way numbers are represented in the programmer's written instructions.)

Let us assume, for simplicity's sake, that there are 1,000 memory "mailboxes," or slots, with addresses ranging from No. 0 through No. 999. Assume further that we are going to use five digits in each program instruction to represent both the operation to be carried out by the computer and the addresses of the slots.

Since three digits are required for the address numbers, two are left to represent the type of operation we want the computer to carry out. Thus, under the above circumstances, a typical instruction would be based on a five-digit number broken down into two parts, as follows:



Bear in mind that the "noun" part of the above information refers to the address number and not to the numbers stored as data at that address. Actually, in designating the address as part of his instruction, the programmer is really interested in the information available at that address.

Getting back to inventories again, let us take the case of a warehouse where we want to keep track of 50 categories of items that are being stocked—with the number of items in each category having a maximum quantity that can be expressed in five digits. At the end of each day we want to know how many items we have left in each category.

For each category, this involves adding new receipts to the quantity originally on hand and subtracting from the sum the day's total withdrawals. Thus, we have a set of three data numbers for 50 categories, making it necessary to use 150 "mailboxes" with five-digit capacities in the computer's memory to store these five-digit parcels of information.

Beginning with the first category, we could place the "starting amount" of items on hand at Address No. 100, the amount of new receipts at Address No. 200 and the total daily withdrawals at Address No. 300. Arithmetically, we must add the information content of Address No. 100 to the content of Address No. 200 and subtract from the total the content of Address No. 300.

With this accomplished, we would like to keep current by putting the result back at Address No. 100.

For the "verb" part of the instructions, let us designate the number 16 for add only, 17 for the reset-to-0 and add 20 for subtract, 07 for store, 30 for transfer and 50 for print. The simplified program instructions, then, could read as follows:

Instructions	Meaning
17 100	Reset to 0 and add the content of Address No. 100 (amount of items on hand) into the accumulator register.
16 200	Add to the above quantity (items on hand) the new receipts, which will be found at Address No. 200
20 300	Subtract total daily withdrawals.
07 100	Store result at Address N. 100.

Each of the instructions to the left above is a five-digit number and the five-digit capacity of any memory slot can store it. The instruction-number groups could be loaded into the "mailboxes" at the addresses beginning at, say, No. 900. Hence we have the following addresses for above instructions:

Addresses	Instructions
900	17 100
901	16 200
902	20 300
903	07 1000

Once the machine is told—by the setting of switches on the computer console—to start executing instructions beginning at Address No. 900, it will do so in sequence, searching Address No. 901 for its next instruction and No. 902 for the one after that, and so on, unless it is told to do otherwise.

If we want the machine to print out the answer after completing the instruction at Address No. 903, we can put the next instruction in No. 904 as follows:

Address	Instruction	Meaning
904	50 1000	Print content of No. 100

Now that one set of items has been processed, we want the computer to go on and do the same job automatically for the other categories of items in the warehouse. After the first category comes the second, so we might be tempted to put an instruction at Address No. 905 telling the computer to go back to Address No. 900 for its next instruction and start the cycle over again for the second category.

Since 30 means transfer, this instruction would read:

Address	Instruction	Meaning
905	30 900	Go back to 900 and start over

But it would be best not to give such an instruction.

For in going back to 900 and proceeding as before to Nos. 901, 902 and

903, the computer would merely be repeating the processing of information concerning the first-category information stored at Address Nos. 100, 200 and 300.

Let us suppose that the second-category information is actually stored at Addresses Nos. 101, 201 and 301.

Thus, the information stored at 900, 901, 902 and 903 must be changed so the instructions will apply to the contents of Address Nos. 101, 201 and 301. This can be accomplished because of the important fact that the instructions themselves are numbers and therefore modifiable arithmetically.

To modify the instruction at Address No. 900, all we have to do is add a 1 to it, and make it read 17 101 instead of 17 100. The same must be done for the instructions stored at Address Nos. 901, 902 and 903.

Consequently, we store a five-digit 1—00001—at some memory address, say Address No. 400.

Then, forgetting about our last instruction for Address No. 905, we write a new one to be inserted in that “mailbox” and place further instructions at succeeding addresses for the purpose of adding the 00001 to the original instructions at Address Nos. 900 through 903.

The add-1 procedure continues until the 50 categories of items have been processed and readouts printed for each category. After the 50th category is processed, the machine would come to a halt if the instructions contained such a command.

As we have dealt with the warehouse inventory problem above, the rather simple arithmetic requirements already have produced a more complex and longer set of instructions than might originally have been imagined. Additional instructions would actually be required to define the format of the printed output, including matters related to margins, column headings, dates, page numberings, and so on.

But take heart.

Remember that the computer itself has the built-in logical power, when properly programmed in a sound source language, to allow us to communicate with it in a language more like our own—whether it be English, or the languages of science, engineering, mathematics or business.

When a source language is used, each source-language statement causes the compiler program for the language to generate sequences of machine-language instructions like those given for the warehouse inventory problem. It is in this

fashion that the computer helps us program our problems.

All this and other even more impressive feats being performed by the modern Analytical engine are wondrous to behold. But a comment by Lady Lovelace in the 1840s about Babbage's machine still holds true of the present-day digital computer:

"The Analytical Engine has no pretensions whatever to *originate* anything. It can do whatever we *know how to order* it to perform."

January 9, 1967

New Shortcut Found for Long Math Proofs

By GINA KOLATA

In a discovery that overturns centuries of mathematical tradition, a group of graduate students and young researchers has discovered a way to check even the longest and most complicated proof by scrutinizing it in just a few spots.

The finding, which some mathematicians say seems almost magical, depends upon transforming the set of logical statements that constitute a proof into a special mathematical form in which any error is so amplified as to be easily detectable.

Using this new result, the researchers have already made a landmark discovery in computer science. They showed that it is impossible to compute even approximate solutions for a large group of practical problems that have long foiled researchers. Even that negative finding is very significant, experts say, because in mathematics, a negative result, showing something is impossible, can be just as important and open just as many new areas of research as a positive one.

The discovery was made by Sanjeev Arora and Madhu Sudan, graduate students at the University of California at Berkeley, Dr. Rajeev Motwani, an assistant professor at Stanford University, and Dr. Carsten Lund and Dr. Mario Szegedy, young computer scientists at A.T.&T. Bell Laboratories. Dr. Motwani, who is the senior member of the group, just turned 30 on March 26.

"With the conventional notion of a proof, you had to check it line by line," said Dr. Michael Sipser, a theoretical computer scientist at the Massachusetts Institute of Technology. "An error might be buried on page 475, line 6. A 'less than or equal to' should have been a 'less than.' That would totally trash the whole proof. But you'd have to dig through the whole thing to find it," Dr. Sipser said. Now, he added, "the new idea is that there is a way to transform any proof so that if there is an error, it appears almost everywhere. I'd say, 'You have a proof? Show me a page.' If there is an error, it will be there."

The finding, which is built on two and a half years of work by leading researchers, is expected to have a profound impact. But because it is so new and unexpected, mathematicians and computer scientists cannot yet predict its scope of application.

"This is philosophically important," said Dr. Mihalis Yannakakis, a theoretical computer scientist at A.T.&T. Bell Laboratories.

Dr. Manuel Blum, a mathematician at the University of California at Berkeley, agreed that the result was "really exciting," with ramifications that were hard to predict. The new verification method can show up errors in calculations as well as in proofs, experts said, and Dr. Blum suggested it could have a role in checking long computer computations.

Dr. Umesh Vazirani, a theoretical computer scientist at the University of California at Berkeley, said that the discovery was "one of the most outstanding in the past decade," because it allowed investigators to decide, almost at a glance, whether it was worthwhile to try to find an approximate solution to a problem they were unable to solve exactly. "As soon as you formulate a problem, you can know if it is intractable," Dr. Vazirani said.

The finding is so recent that it has not yet been published. "We just wrote it in the last month or so," Dr. Motwani said. As is the custom in mathematics and theoretical computer science, the result gains credibility not by having been sent to a journal and reviewed by other scientists but by having been vouched for by leaders in the field. In this case, at least a dozen experts say they are convinced by the result, and amazed by it.

High Praise for Discovery

"It is absolutely stunning," said Dr. László Babai, a theoretical computer scientist at the University of Chicago whose work helped lay the groundwork for the new discovery.

Dr. Richard Karp, a theoretical computer scientist at the University of California at Berkeley agreed. "Personally, to me it's very surprising," he said. Dr. Karp added that the method's application to show that certain problems have no approximate solutions is the most important discovery in his field of theoretical computer science in more than two decades.

The insight into the nature of proofs shows how a connection can be created between each and every logical statement of a proof, no matter how long or complicated the proof may be. It applies to the 15,000-page proof that is the longest ever published as well as to the single-sentence proof that can be grasped in an instant. And it is no harder to check a long proof than a short one. "Even if your proof is the size of the universe, you still would not have an increased number of places to check," Dr. Babai said.

The investigators used a variety of mathematical tricks to transform a proof so that its errors, if any, will show up almost everywhere. One method they used was a way of comparing lists of data.

Data comparisons are an integral part of long proofs. For example, Dr. Babai pointed out, a typical mathematical proof might have a line that says, "We know by theorem 31 that $a = b$ and by theorem 72 that $b = c$. Therefore, we conclude that $a = c$." To see if this statement is correct, Dr. Babai said, "We have to go back to theorem 31 and see that it does indeed say $b = c$, and similarly we have to look up theorem 72 and see that it has been copied correctly."

One way to compare two lists of numbers is to arrange them in a grid and then extend each row and column in an arithmetic progression. To compare the data list 1,3,-1,4 with 1,5,-1,4, in which a single digit has been miscopied, the lists would be formed into arrays with 1,3 and 1,5 in the top rows. The rows would then be extended in arithmetic progression, forming 1,3,5,7,9,11 and 1,5,7,9,11,13. Already the one-digit difference has been amplified to five differences.

By increasing the number of items listed in the arrays, the number of differences in an extended array can be made so great that sampling just a few squares will be bound to detect a difference and thus an error in one of the original data sets.

Inherent Uncertainty

Proofs are not data but they can be manipulated in analogous ways by representing each step of a proof as a term in a mathematical equation. For example, Mr. Arora said, a logical statement in a typical proof might say "either statement x and statement y are true, or statement z is not true." This can be converted to the equation, $xy + (1 - z)$.

Using these equations, the mathematicians formulated relationships that would have to hold if the proof contained no error.

Dr. Blum said that the new finding does have in it an intrinsic uncertainty. An error will show up in almost everywhere in a suitably transformed proof, but not absolutely everywhere. But, he said, it is easy to probe the proof in enough places to make the chance of missing the error negligible.

"Realistically, you can make the probability of missing an error as small as 1 divided by the number of atoms in the universe," Dr. Blum said. That means you can make the chance of mistaking an incorrect proof for a correct one, "virtually zero," he said.

The investigators also noticed that their proof was mathematically equivalent to a profound statement of how difficult it would be to solve certain problems that plague mathematicians. Their proof about proofs showed that it was just as hard to get an approximate solution to a class of very hard problems as it was to get an exact solution. Since computer scientists have pretty much given up on exact solutions to these problems, the new result means they must abandon even their remaining shreds of hope of obtaining rough solutions to a wide group of practical problems.

Widely Pondered Problems

This group of thousands of problems involves finding the best ways to do things like design telephone networks or airline routes or to set up sequences of jobs in factories. Although no one has ever proved that an exact solution is impossible, the consensus is that they are. Dr. Babai said mathematicians had tried for centuries to find an exact solution, to no avail. "Literally thousands of people have considered these problems, including the greatest minds in mathematics, including Gauss, and have gotten nowhere," he said, referring to Carl F. Gauss, an 18th-century German mathematician and astronomer.

In 1971, investigators showed that a wide range of these very hard problems were mathematically equivalent: a solution to one would solve all. Without hope of an exact solution that would solve them all the time, they began a search for an approximate solution that would always come very close, at least, to the best answer.

Dr. Babai explained: "There was a feeling that, 'All right, we are not interested in the best possible solution. If we can get within 1 percent of an exact solution, that's good enough.'" Investigators found some good approximate solutions that worked for some problems some of the time, but they could not find a good approximation that would always work. Now they know there is a reason for that. The solutions they were seeking were as hard to find as exact solutions.

Dr. Karp said this finding alone was a monumental achievement, equivalent in its impact to the finding in 1971 that the problems were equivalent. Until now, he said, "One could always cling to the hope that one could get what one wanted with a fast algorithm that gives a good approximation. Now we know that even that is unachievable."

April 7, 1992

New Technique Stores Images More Efficiently

By GINA KOLATA

Engineers devising new methods of storing information electronically have long used as their standard test the photograph of a certain young woman. She is wearing a floppy straw hat with a feather on it. She is gazing over her right shoulder with a sultry expression. And her dark hair is cascading down on either side of her face.

The trick is to put the minimum amount of information needed to reconstruct that photograph into a computer and then pull it back out. And the problem has been that when the picture was reconstructed, the feathers on the hat were blurry, or a strand of hair was indistinct or a highlight in the right eye was lost. Or, in many cases, it took too much data to reconstruct a clear image.

But now mathematicians and engineers have devised a new way to compress data that passes this photograph test with flying colors and, they say, it may revolutionize the world of information storage and retrieval.

Researchers say the method, called wavelets, can provide clearer sound transmission and more bands for cellular telephones and better images for high-definition television. In addition, it should make it possible to compress data that people thought could not be squeezed without loss of crucial details. The new method can also help mathematicians solve matrix equations, involving enormous rows and columns of numbers, by allowing them to transform the equations into simpler forms.

The wavelets method appears to resemble the way the human eye and human ear process data. The eye essentially computes the difference between blurry images to find places where there are lines or edges, said Dr. Ronald Coifman, a mathematician at Yale University. Wavelets provide a similar array of blurry images that when pieced together, gives a clear picture. And just as the ear hears in octaves, wavelet analysis also splits sound frequencies into octaves for storage, Dr. Coifman said.

Dr. Victor Wickerhauser of Washington University in St. Louis said mathematicians and engineers were "so excited by wavelets they are using them for everything under the sun." And Dr. Howard L. Resnikoff, president of Aware Inc., which makes a wavelet computer chip, said the wavelet discovery was so important that it was "one of the mathematical events of this century."

Because the method is so new, it is not yet appearing in commercial applications. But researchers say that is about to change. At A.T.&T. Bell Laboratories, for example, researchers are using wavelets to compress speech. And Dr. Wickerhauser is using them to reproduce music without noise or distortion.

A Tricky Problem

The problem of compressing data is trickier than it appears at first. Previous methods have either required too much computer storage space, taken too much time or sacrificed precious detail in storing the data. For that reason, some groups decided that they were simply unable to store their data in computers, no matter how urgently they needed to enter the computer age.

For example, weather photographs from orbiting satellites are transmitted to earth without any attempt at compressing the data, Dr. Wickerhauser said. He explained that it was so expensive just to get the data that the scientists did not want to take any risk of losing precious parts of it.

At the Federal Bureau of Investigation, fingerprints are still stored on cards kept in a cavernous room in Washington. But the agency has 25 million fingerprint cards and its files grow by thousands of cards a day as new criminal suspects are fingerprinted.

Like the scientists with their satellite data, the F.B.I. felt it could not afford to lose any details as a result of electronically compressing the data on a card for storage in a computer. But, said Thomas Hopper, the director of the bureau's quest to put its fingerprint files on computers, if the agency stored every detail, without alteration, the data from just a few cards would require as much storage space as is on a hard disk of a personal computer. If the agency wanted to transmit all the data on a fingerprint card over a telephone line, it would take 18.5 hours at the standard transmission rate of 1,200 baud, Mr. Hopper said.

F.B.I. Is Interested

Mr. Hopper and his colleagues at the bureau have now become seriously interested in wavelets. They have consulted extensively with Dr. Wickerhauser and others who say that the method can store fingerprints compactly, allow them to be transmitted easily and allow the details of the fingerprints to reappear when the computer data are reverted back to a picture.

To compress data, the problem is to find simple mathematical equations that describe the data at each point. Rather than trying to store every dot of a bell curve in a computer, for example, a mathematician could write a few symbols of an equation that, when graphed, reproduces that curve.

But the situation gets more complicated when the image to be stored is not just a simple curve but is a photograph or a fingerprint or a sound pattern. At each point of a photograph, for example, there are data telling the color at that point and where it is in the picture.

Rather than store an entire array of data, each point telling color and position, it should be possible to devise equations that describe that information. As the picture gets more detailed, each tiny segment can be modeled by a greater number of equations that added together and graphed will reproduce the picture. But with very complex pictures or sounds, the equations that are needed can get ever more cumbersome and their ability to fit the picture ever poorer.

A Tinkertoy Analogy

Dr. Coifman likens data compression to building with a set of Tinkertoys and trying to model an ornate building. With traditional methods, he said, "you have a Tinkertoy and are trying to build something out of it, but the shape of the toy may not be the shape of what you are trying to build," he said.

Wavelets, he added, "provide a whole new collection of Tinkertoys," adding, "For one task, you might choose one collection of them and for another task you will pick another collection." As a result, investigators can come much closer to modeling exactly what they want with as few equations as possible.

The first paper showing that wavelets could be a practical tool was published in 1988. But the wavelet story began several years earlier, when a French geophysicist, Dr. Jean Morlet, devised an ad hoc method to help find oil deposits underground.

Geologists do this by shooting sound waves into the earth and listening to the echoes to try to determine the shapes of underground structures that could have produced those sound patterns. The task is like trying to determine the shape of an object from the shadow it casts, a longstanding problem that has been well studied.

Dr. Morlet, who worked for Elf Aquitaine, knew the classical way to solve the problem: model the process with a set of sine and cosine curves. This

method, known as Fourier analysis, has been around for more than a century and is an indispensable tool. The smooth, undulating sine and cosine waves can be arranged so that, when enough of them are added together, they converge to match the shape of any given curve.

But the sine and cosine curves also overshoot and undershoot the curves that are to be modeled, so Dr. Morlet decided to make a set of more precisely tailored curves to better fit the data. The idea was to fit graphs of equations with simple humps and bumps that can be more peaked or spread out and can start or stop whenever needed. By writing equations to describe a set of overlapping simple curves, it should be possible to mimic closely the much more complex graphs that defied Fourier analysis, Dr. Morlet reasoned. He called his set of simple curves wavelets.

When Dr. Yves Meyer, a mathematician at Paris Dauphine University, learned about Dr. Morlet's work, he immediately realized that wavelet theory was actually part of the mathematics of harmonic analysis, a field of pure mathematics that had been studied for its intrinsic abstract beauty. It turned out that mathematicians had already laid the necessary theoretical groundwork for wavelets analysis.

Using harmonic analysis theory, Dr. Meyer constructed a family of wavelets that he proved were the most efficient family for modeling most complex phenomena. But Dr. Ingrid Daubechies of A.T.&T. Bell Laboratories, who has worked with Dr. Meyer, said the proof did not provide the necessary intuition that investigators needed if they were to make full use of wavelets.

A Need for Miracles

"The proof was clear, you could read it, but it seemed like it needed miracles happening," Dr. Daubechies said. "The idea was that something very deep was happening, but, reading the proof, you couldn't understand why."

The intuition came from Dr. Stéphane Mallat, an engineer who is now at New York University. "When I began to look at what Meyer had done," Dr. Mallat said, "I realized it was very close to some ideas in image processing. Suppose you have an image of a house. If you want to recognize simply that it is a house, you do not need most of the details. So people in image processing had the idea of approaching the images at different resolutions."

Using that idea, Dr. Mallat developed a family of wavelets to use to describe any image. He explained that he decomposed the original image into a pile of

images at increasingly detailed resolutions. Each image of the pile is described with wavelets. If all the images are put together, the original image in all its detail pops out. If not so much detail is needed, some of the wavelets need not be used.

Dr. Daubechies carried the idea one step further and published a simple collection of wavelets that she proved were the most efficient. Her paper, researchers said, was just what was needed to make wavelets practical.

Dr. Daubechies said she had focused on compressing data in photographs, storing enough to reconstruct the exact image with the minimum number of wavelets. She has now reduced the amount of data she must store to one 40th of the amount that would be needed with other methods, like Fourier analysis.

She said the method could be used by hospitals to store X-rays. A doctor could scan X-ray photos that were reconstructed very quickly with coarse detail. When the doctor finds X-rays he wants to examine more closely, he can have the computer do additional calculations, adding in more of the wavelets used to store the data, and reconstruct an exact facsimile of the original photo.

Dr. Wickerhauser is using wavelets to store human speech compactly. He said the advantage of wavelets was that unlike other methods, they did not magnify background noises.

Use of Weather Satellites

Another application, Dr. Wickerhauser said, is storing data for weather satellites. So far, satellite data have not been compressed, but Dr. Wickerhauser said, "the amount of data that are going to be transmitted from space in the near future is so huge that there will be both a transmission and a storage problem."

With wavelets, he said, researchers can zero in on the data that are relevant and use them to predict weather patterns. For example, to follow a hurricane, they may need to track only hurricane clouds, something that can easily be done by picking out these clouds alone from the data stored with wavelets.

Dr. Coifman said the final story of wavelets' impact had yet to be written. He said the technique had "opened the door for a new kind of analysis." And, he added, at this point, "it is the opening that makes it exciting."

November 12, 1991

Giant Computer Virtually Conquers Space and Time

By GEORGE JOHNSON

Janus, recently christened the world's fastest supercomputer, is not much to look at: 84 tall gray cabinets resembling plastic gym lockers lined up inside a claustrophobic, fluorescent-lighted room.

Inside the drab enclosures, 9,072 Pentium Pro processors silently trade information, giving the computer, built by the Intel Corporation and installed this summer at Sandia National Laboratories here, the power to perform a once-inconceivable trillion mathematical operations per second.

Overhead the blowers for the cooling system roar, carrying away the tremendous heat generated by squeezing so many calculations into a tiny sliver of time. The noise is the sign that behind Janus's lifeless facade, an enormous amount of computational labor is being done. Computing power has increased so rapidly over the years that the announcement of yet another world's fastest supercomputer seems almost routine. Supercomputers are rated according to how many mathematical operations, like multiplying two numbers, they can do in a single second. Since these tasks involve keeping track of the position of the decimal point, they are called floating point operations, or flops.

Over the years, megaflop machines, performing millions of operations a second, have given way to gigaflop machines, performing as many as hundreds of billions. The new computer at Sandia is the first teraflop machine. Tera means trillion, and by crossing this threshold, computer science has made a qualitative leap in the ability to use information to model the world.

Janus is so fast and has so much memory (hundreds of billions of bytes, compared with millions in a typical personal computer) that it can simulate complex events—like explosions, nuclear fusion reactions, missile impacts or the crash of a comet into the Earth—with a fineness of detail that was impossible before.

"The increase in power has almost no precedent," said Dr. William J. Camp, director of computational science, computer science and mathematics at Sandia. "In one fell swoop, we've raised computing power by an order of magnitude."

When scientists re-create biological reactions in a test tube, they say they are working "in vitro," from the Latin word for glass. Experiments carried out inside the silicon chips of a computer are done "in silica." While two-dimensional

simulations are now commonplace, adding the third dimension takes an enormous amount of additional computer power. Rendering a three-dimensional process in fine detail, and then having it unfold along the fourth dimension, time, strains even the most powerful computers.

In 1970, Dr. Camp said, supercomputers could roughly simulate a clump of matter consisting of a thousand atoms and follow its behavior for about a nanosecond, a billionth of a second. Re-creating this brief moment took those computers a few hours of intense calculation. In about the same time, Dr. Camp said, the teraflop machine can follow 100 million atoms for as long as a microsecond, a millionth of a second—an eternity on the atomic scale.

The new teraflop machine was ordered for the federal Department of Energy's Accelerated Strategic Computing Initiative, which tries to use simulations to test nuclear weapons without the environmental and political risks of exploding them in the real world.

"For the first time we can do full four-dimensional simulations," Dr. Camp said. "That's really a qualitative change." In the past, he said, weapons simulations were not detailed enough to substitute for real testing.

Researchers at Sandia, a Department of Energy lab, recently used Janus to mimic a ballistic missile strike. For the missile to explode, the triggering mechanism must survive the initial impact and, a moment later, set off the explosion. By sifting through the simulated wreckage on a computer screen, scientists could see whether the missile was correctly designed. The accuracy of such models, of course, is only as good as the assumptions built in. But the teraflop computer allows scientists to play out the consequences of their theories with unprecedented precision.

The computer at Sandia is not used only for weapons work. It is nicknamed Janus because, like the Roman god, it has two faces: one side of the computer can be used for classified research while the other is solving unclassified problems.

Scientists recently used the teraflop computer to simulate the split-second timing of a nuclear fusion experiment. Janus was also used to analyze what would happen if a comet a kilometer, or about six-tenths of a mile, in diameter and weighing about a billion tons struck the Earth's atmosphere, vaporizing part of the ocean and setting off tidal waves.

"This is an experiment I would not want to witness firsthand," said Dr. Mark Boslough, a physicist at Sandia who worked on the comet project. "The simulation enhances our insight and understanding of the physics of big impacts in a way that would not be possible by any other means."

Dr. Boslough said that at teraflop speeds, computer simulation is coming into its own as a new way to do science. "Until recently, scientists have described themselves as either experimentalists or theorists," he said, "but computational science is rapidly establishing itself as a third branch of inquiry, and the one that is the most likely to lead to the next major breakthroughs in many areas of research."

Computers are becoming so powerful that scientists say they must remind themselves not to confuse the simulation with the real thing. "Supercomputer simulations greatly enhance, but will never eliminate the more traditional way of doing science," Dr. Boslough said. "Without a good experimental and theoretical foundation, it would just be garbage-in, garbage-out—trillions of times per second."

The data-intensive nature of these high-fidelity virtual experiments is already stretching the new machine at Sandia to the limit. The number-crunching required to follow the missile impact for a mere 100 microseconds took five days. The smallest detail that could be rendered was on the millimeter scale. Seeing what would happen to the missile's smaller parts would take a finer-grained simulation, and that would require more computing power.

In the next few years, Janus will be joined by two more teraflop machines at other Energy Department labs. The Los Alamos National Laboratory in New Mexico is scheduled to get a supercomputer built by Silicon Graphics Inc., and the Lawrence Livermore National Laboratory in California will get one built by the International Business Machines Corporation. All three will be connected to form a network of vast computational power.

In the old days of supercomputing, all the data being manipulated had to be funneled through a single processor, a custom-made product that for its day was state of the art. The new generation of supercomputers uses a parallel architecture in which thousands of off-the-shelf components, like the commonplace Pentium Pro processors, are harnessed to work on a problem simultaneously.

The logistics of coordinating all these interacting chips is like conducting a symphony, said Dr. Gyan Bhanot, a researcher at I.B.M.'s Thomas J. Watson Research Center in Yorktown Heights, N.Y. "There may be a lot of music," he said, "but it is just noise unless a conductor is there to orchestrate everything."

For years scientists have wondered how far they can push the limits of computation. Signals in a computer can travel no faster than light. So the faster a computer becomes, the closer its components must be to one another. Otherwise the

signals would not reach their destinations within the rapid ticks of the computer's internal clock. And the closer the components are, the harder it is to keep them from frying in their own heat.

Squeezing ever more parts onto each silicon chip also requires etching finer and finer wires to connect them. Carried by vanishingly thin conduits, the data are more likely to be scrambled by the ubiquitous random vibrations called thermal noise. To insure the integrity of the calculation, more error-correcting circuitry must be installed. And that means more components to squeeze together and more heat to overcome.

Still, there seems to be no immediate end in sight. "We are not even close to pushing the fundamental limits in the foreseeable future," said Dr. Rolf Landauer, a scientist at the Watson Research Center. "The real limits come from money, not physics."

Scientists hope to speed up computers like Janus a hundred times by 2005. And they hope to multiply the speed a thousandfold by 2010, resulting in the first petaflop machine. In a single second it would carry out a quadrillion (a thousand trillion) operations.

Dr. Bhanot said a petaflop machine could conceivably be built today. But the speed is not the only factor that would be a thousand times greater—so would the price. Janus cost \$55 million to make. "Today we could build a petaflop machine if we had \$55 billion," he said. "No problem. But not even Bill Gates could afford this." In 10 years, he predicted, the cost will be down to about \$55 million, and by that time the lumbering teraflop computers will be commonplace.

When the petaflop era arrives, the gap between simulation and reality will become that much narrower.

Justin Rattner, an Intel fellow at the company's supercomputing plant in Beaverton, Ore., said: "Each step up in computing power takes you that much closer to considering all the known physics, chemistry and thermodynamics for a given physical phenomenon. At petaflop speeds, we should be very close to modeling nature, at least as we know it, with a very small degree of error.

"Experiments that are simply unthinkable in physical terms can and will be conducted on and by these computers," Mr. Rattner said. "Imagine being able to stop the universe a few femtoseconds after the Big Bang and just poke around to see what's happening." A femtosecond is one-quadrillionth of a second. "Or imagine watching the folding of a protein at an armchair pace," he said. "These and many other opportunities await us."

Is there any end to the increase in power? The need to use smaller components in order to achieve faster speeds suggests a possible barrier: miniaturization, it seems, would have to stop when the parts of a computer were as small as a single atom. But perhaps, Dr. Landauer speculates, one could make a computer whose components were subatomic particles: pieces of atoms.

Beyond that, he said, there is one obvious barrier that probably cannot be overcome. "The size of the universe is a limit," Dr. Landauer said. "It determines the maximum size of the memory I can put together."

Make the computer too big and it will have nothing to think about except itself.

September 2, 1997

Rear Adm. Grace M. Hopper Dies; Innovator in Computers Was 85

By JOHN MARKOFF

Rear Adm. Grace Murray Hopper, retired, a mathematician and pioneer in data processing who was a legendary figure among both computer scientists and industry executives, died New Year's Day at her home in Arlington, Va.

Admiral Hopper, who was 85 years old, had been in ill health recently, family members said, and died in her sleep, apparently of natural causes.

She had been in the Navy, as an active-duty officer or a reservist, since World War II, and received a special presidential appointment to the rank of rear admiral in 1983. In 1982, with the retirement of Adm. Hyman J. Rickover, Admiral Hopper became the oldest officer on active duty in the armed service, which she remained until retiring herself in 1986.

Admiral Hopper made several vital contributions to the development of modern computing systems, including helping invent the COBOL programming language, which is still in widespread use in business.

Award from President

In September, President George Bush awarded her the National Medal of Technology "for her pioneering accomplishments in the development of computer programming languages that simplified computer technology and opened the door to a significantly larger universe of users." She was the first woman to receive the award individually.

At the time of her death she was a senior consultant to the Digital Equipment Corporation. She joined Digital in 1986, shortly after her retirement from the Navy.

"Grace took every opportunity to challenge people young and old to consider the infinite possibilities of technology," said Kenneth H. Olsen, Digital Equipment's president.

Admiral Hopper was born Grace Brewster Murray on Dec. 9, 1906, in New York City. After receiving a Ph.D. in mathematics from Yale, she taught math at Vassar College, her alma mater, where she later became an associate professor. She was divorced in 1945 but kept her married name.

In 1949 she worked as a mathematician at the Eckert-Mauchly Corporation. The company was formed by Dr. John W. Mauchly and J. Presper Eckert, who in 1946 had developed one of the world's first electronic computers, ENIAC, at the University of Pennsylvania. Eckert-Mauchly was then building the UNIVAC I, the first commercial electronic computer. The company was later bought by the Remington Rand Corporation.

Earlier, in 1943, Dr. Hopper had joined the Navy. As a lieutenant assigned to the Bureau of Ordnance Computation Project at Harvard University, she worked as a programmer on a calculating device called the Mark I, a precursor to electronic computers.

Recalled by the Navy

Leaving the Navy in 1946, she remained at Harvard as a faculty member in the computation laboratory. She continued to work on early Navy computers and maintained her Naval career as a reservist. Although retired from the Navy reserve in 1966, then-Commander Hopper was recalled within a year to active duty to oversee a program to standardize the Navy's computer programs and languages.

In 1962, she was elected a fellow of the Institute of Electrical and Electronic Engineers. In 1969, the Data Processing Management Association selected her as its first computer sciences "Man of the Year."

Her work led to the first practical compiler for modern computers. A compiler is a program that translates instructions written by a human programmer into more specific codes that can be directly read by a computer.

Among her many contributions, Admiral Hopper is known for coining the term "bug," which is widely used to refer to mysterious computer failures.

The first bug actually was—a moth, as Admiral Hopper told the story. It was discovered one August night at Harvard in 1945 inside the Mark I.

"Things were going badly, there was something wrong in one of the circuits of the long, glass-enclosed computer," she is quoted as saying. "Finally, someone located the trouble spot and, using ordinary tweezers, removed the problem, a two-inch moth. From then on, when anything went wrong with a computer, we said it had bugs in it."

Like another Navy figure, Admiral Rickover, Admiral Hopper was known for her combative personality and her unorthodox approach.

A self-described "boat rocker," she once said in a speech that she hoped to live until the year 2000. "I have two reasons," she said. "The first is that the party on Dec. 31, 1999, will be a New Year's Eve party to end all New Year's Eve parties. The second is that I want to point back to the early days of computers and say to all the doubters, 'See? We told you the computer could do all that.'"

She is survived by a brother, Dr. Roger F. Murray II of New Hampshire, and a sister, Mary Murray Westcote of New Jersey.

January 3, 1992

Frances E. Holberton, 84, Early Computer Programmer

By STEVE LOHR

Frances Elizabeth Holberton, one of the first computer programmers, whose contributions to software over the years ranged from an early data-sorting program to helping develop the business programming language COBOL, died on Dec. 8 at a nursing home in Rockville, Md. She was 84.

The cause was heart disease, diabetes and complications from a stroke that she suffered several years ago, according to her daughter, Priscilla Holberton of Silver Spring, Md.

"Betty Holberton was a real software pioneer," said Donald E. Knuth, a professor emeritus at Stanford University and author of the three-volume *The Art of Computer Programming*, the profession's defining treatise.

Mrs. Holberton, a graduate of the University of Pennsylvania, was one of the six young women recruited by the Army to program the Electronic Numerical Integrator and Computer, which became known by its evocative acronym, ENIAC. The ENIAC is credited with being the first all-electronic digital computer.

The ENIAC's job was to calculate the firing trajectories for artillery shells. The young women programmers were selected for their skills in mathematics. The work they did was "hard-wired" programming, laboriously setting switches and cables inside the 30-ton black behemoth of a machine.

Mrs. Holberton, colleagues recall, was particularly adept at figuring out the best path for guiding the complex calculations through the electronic labyrinth of the ENIAC. Frequently, these insights came to her overnight.

"Betty had an amazing logical mind, and she solved more problems in her sleep than other people did awake," recalled Jean J. Bartik, another of the ENIAC programmers.

The ENIAC was demonstrated in February 1946, too late for use in World War II, but it helped open the door to modern computing. The ENIAC programming team broke up, but Mrs. Holberton was the one of the six who stayed longest in the field.

After the war, she joined the ENIAC designers, John Presper Eckert and John W. Mauchly, in their effort to develop the UNIVAC, an early commercial computer, which was introduced in 1951. While working on the UNIVAC, Mrs.

Holberton did some of her most innovative work. She developed a program for sorting and merging large data files, which at the time were stored on reels of magnetic tape. Any such updating of data files was an arduous programming task at the time, and her program vastly simplified that job.

"That was a huge tour de force," said Paul E. Ceruzzi, a computer historian at the Smithsonian Institution.

In 1953, Mrs. Holberton joined the Navy's Applied Math Lab at the David Taylor Model Basin in Maryland as the supervisor of advanced programming, where she worked until 1966. In 1959, she was a crucial member of the committee that developed COBOL, or Common Business Oriented Language. The committee worked for six months on the standards and specifications for a business programming language, which was introduced in 1960.

The committee's work was seen as a temporary solution to the growing problem created by the increasing need for a standard programming language for handling business data at a time when computing was moving into the mainstream of the corporate world. Yet COBOL, updated many times over the years, is still widely used.

Computer scientists often criticize COBOL as a hasty, inelegantly designed programming language. But it gave computing a way to handle and visually describe business data, making it easier to program business problems on computers.

Mrs. Holberton, who joined the National Bureau of Standards in 1966 and worked there for two decades, once echoed those views. In a 1983 interview conducted for the Charles Babbage Institute, a computing history center at the University of Minnesota, Mrs. Holberton conceded some of the criticisms of the language she helped develop. But, she added, "COBOL, I felt, was very important because of its ability to describe data."

According to Kathryn Kleiman, a lawyer who is working on a documentary film on the women in the ENIAC program and their contribution to the field, Mrs. Holberton consistently worked on trying to make computers easier to program.

"She took that hard-won knowledge on the ENIAC and applied it over the next 40 years, in nearly everything she did in the field," Ms. Kleiman said.

In addition the her daughter Priscilla, Mrs. Holberton is survived by her husband, John Vaughn Holberton, and another daughter, Pamela Holberton, both of Rockville.

December 17, 2001

Squeezing Data like an Accordion

By PETER WAYNER

Most software packages offer their users the chance to use compression to save disk space and make downloads faster. But what is compression? It's a shorthand system that computers use to save space. In other words, it's like lingo, buzzwords or telegramspeak—short abbreviations people adopt to save words.

Understanding “compression” begins with understanding “information” because the two are linked. Computers try to compress files by boiling them down to their essential information. But anyone sitting in a committee meeting knows that can be a difficult and perhaps impossible task.

Many theoretical insights into compression came in the late 1940s when Claude Shannon worked for Bell Labs and developed a theory of information. He created a mathematical model that measured information by its surprise value. Unexpected data has more information in it than data that falls into a regular pattern, he said. One side effect was that this work provided the insight into building optimal mathematical tools, or algorithms, to achieve compression.

While finding that the ultimate compression system is probably impossible, many programmers have come up with fairly good approximations. Most systems scan a file to identify common patterns of letters, numbers or data, then come up with a shorthand system to represent these common patterns in a smaller amount of space. Some of these systems are tuned to particular types of data, like images or video or sound files, and others will work with all forms of data.

Two of the general compression systems that emerged from this era are known as Huffman coding and Lempel-Ziv compression. Many more recent solutions like PKZIP are variations on these algorithms. Instead of describing these more modern systems in detail, it is easier to describe some of their earlier precursors, from the telegraph era, that also used the same basic ideas.

One of the principal notions is to use short code words for the most common patterns and longer ones for the less frequent patterns. That idea was used in Morse code, which assigned short codes for common letters (like E equals dot and T equals a dash) and long codes (like P equals dot-dash-dash-dot) for less common letters. In Huffman coding, an option used by most of the major compression software packages, a table is made of the common letter patterns, which are assigned to short patterns of ones and zeros.

Of course, these solutions produce results that depend upon the data being compressed. English text will usually be reduced about 50 percent to 70 percent by Huffman coding, but the results depend upon the writer and the data. If there is plenty of repetition and cliches, then Huffman coding can usually identify more common passages and save more space by assigning shorthand representations for these common phrases. On an intuitive level, it should be easy to see that the less information a document has, the more compression that can be done. Dr. Shannon formalized that idea with mathematics.

Another common technique is known as the dictionary method; the Lempel-Ziv solution is a variation of that general class. Again, this idea was often used when sending telegrams. In the early part of this century, companies competed to create code books for each industry, assigning numbers to common phrases from each type of business.

In telecommunications, for instance, ZDH is a shorthand for your dits are too heavy, please adjust, WX is shorthand for weather, and XMTR means "transmitter."

In the telegram era, both sides needed copies of the same code book. The Lempel-Ziv solution includes a way to incorporate a copy of a code book suited for a particular file into the final compressed version of the file. One for this article would probably include words like common and compression at the top of the list.

Other compression algorithms are tuned to particular types of data. The Joint Photographic Experts Group, or JPEG, solution can compress photographs to one-hundredth of their original size, although the images often lose resolution in the process because some information about the image is lost. The solution trades off compression for image quality. Less compression means that more information is left in the file and less damage is done to the image. Art directors who use the JPEG method to compress images put on the Web often check out different levels of compression to see just how bad the damage is. Sometimes it even makes the images look better.

Solutions like JPEG and its moving picture cousin called MPEG are hard to describe without using words like cosine, but a simpler version can explain how some solutions are adapted for particular classes of data. Black and white line drawings, for instance, can often be compressed significantly with a solution known as run length encoding. That consists of going through the image pixel by pixel and counting the number of times that each type of pixel is repeated. A pattern like black black black black white white would be compressed to B4,W2

and, starting with white, "white white white black black" to W3,B2. That works quite well on line drawings with big blocks of black or white because many pixels can be boiled down to one entry.

Of course, people are getting better at boiling down long passages of text into their essential information. An episode of the television series *Seinfeld* revolved around how some characters would make a long story short by sliding past the extra details with the phrase yada, yada, yada. That is, they cut to the chase, yada, yada, yada.

June 18, 1998

A Digital Brain Makes Connections

By ANNE EISENBERG

The ability to recognize patterns—the way noses tend to appear in the middle of faces, how words like “throw” are often associated with “curve ball” and “touchdown pass”—has always been linked with human intelligence. Not necessarily high intelligence, but something that machines have a hard time with.

In the process of investigating how the brain might accomplish such impressive feats, two physicists have devised a novel program that can recognize the existence of patterns, although it cannot yet figure out what they mean.

Their creation, a learning algorithm, may one day inspire not only better searches on the Web, but also wide-ranging improvements in computer applications like voice recognition and medical imaging and other applications that call for a computer to parse a mass of complex data.

The algorithm, a math-based strategy, was developed by Sebastian Seung, an assistant professor in computational neuroscience at the Massachusetts Institute of Technology, and Daniel Lee, a researcher in the biological computation department at Bell Labs, the research and development arm of Lucent Technologies in Murray Hill, N.J. Their account appears in the Oct. 21 issue of the journal *Nature*.

“Our method seeks to imitate the way in which we think the brain uses patterns to make sense of the world,” Dr. Seung said.

The two physicists, part of the community of scientists working on the border of artificial intelligence and neuroscience, tested their learning algorithm with images and with words. For images, they gave it pictures of faces. For words, the algorithm was provided with encyclopedia articles. The job was the same: to find recurring pieces of text or images and put them into groups.

The algorithm works by the statistical analysis of words or pixels that occur together and that may therefore be related. For faces, the algorithm looked for pixels that repeatedly popped up together.

“It was not looking specifically for noses but for repeated patterns,” Dr. Seung said. “We didn’t explain about noses.” On its own the program came up with groups that quite visibly resembled noses, mouths or other features constituting identifiable facial parts.

For text, the algorithm grouped words like “flower,” “leaves,” “plant” and “perennial” together. Once the groups were created, the researchers labeled them as belonging to a topic, like botany.

The method for identifying images of facial parts or topics in text relied on using the algorithm to analyze huge amounts of data: volumes of an encyclopedia and thousands of faces. “It’s surprising what you can discover about meaning from statistics, that is, essentially from what gets used together,” Dr. Seung said.

Dr. Lee emphasized that the researchers’ learning algorithm worked without supervision. They did not tell the algorithm which features constituted a face, for instance, or where to look for items that might belong in the category “botany.” “Much of human learning is done without a teacher around,” Dr. Lee said. “We wanted an algorithm that could in an unsupervised fashion recognize correlations.”

An artificial-intelligence expert, Geoffrey Hinton, director of the Gatsby Computational Neuroscience Unit of University College, London, said Dr. Seung and Dr. Lee’s approach was an important contribution.

“It’s a novel way of taking large data sets and automatically finding features,” Dr. Hinton said.

The new approach may also lead to valuable information on how the brain extracts features from images, Dr. Hinton said. People can become very good at doing that, he said, using as an example someone who was an expert reader of X-rays.

“People learn over several years to see details in X-rays that they could not initially perceive,” Dr. Hinton said. But it is not clear how the brain works to increase this skill.

“When we understand how the brain extracts different features,” Dr. Hinton added, “we can make computer vision systems that are better at interpreting medical images.”

At A.T.&T. Laboratories in Florham Park, N.J., Dr. Fernando C. N. Pereira, head of machine learning and information retrieval research, confronts problems related not to how the brain processes images but to how it handles language. “This is an important advance,” he said of the new approach. “It brings together two seemingly separate areas—images and language—and shows that they can be subsumed under one single model.”

Dr. Pereira, an expert in language processing, said one of the most challenging problems in the field was determining how people learn certain cues that help them understand language.

"Children learning language may draw from words and sentences in context to get meaning, plus they also have other cues from seeing and hearing," he said.

Computers, in contrast, do not yet have this rich sensory capability to draw on when confronted with the language used in daily life.

Like Dr. Lee and Dr. Seung, Dr. Pereira analyzes acres of text, using statistical methods to find indicators of the meaning that words have in context.

"As we build better models of how the underlying structures of speech and text are learned," he said, "we can apply them to speech recognition and information retrieval."

Dr. Pereira avoids the word "understand" when he talks about the models he is developing that help computers handle human speech and text.

"My work is in having computers process and react appropriately to natural-language speech and text," he said. "The term 'understanding' turns out to be too controversial. I'm settling for 'react more appropriately.'"

November 4, 1999

A Soviet Discovery Rocks World of Mathematics

By MALCOLM W. BROWNE

A surprise discovery by an obscure Soviet mathematician has rocked the world of mathematics and computer analysis, and experts have begun exploring its practical applications.

Mathematicians describe the discovery of L.G. Khachiyan as a method by which computers can find guaranteed solutions to a class of very difficult problems that have hitherto been tackled on a kind of hit-or-miss basis.

Apart from its profound theoretical interest, the discovery may be applicable in weather prediction, complicated industrial processes, petroleum refining, the scheduling of workers at large factories, secret codes and many other things.

"I have been deluged with calls from virtually every department of government for an interpretation of the significance of this," a leading expert on computer methods, Dr. George B. Dantzig of Stanford University, said in an interview.

The solution of mathematical problems by computer must be broken down into a series of steps. One class of problem sometimes involves so many steps that it could take billions of years to compute.

The Russian discovery offers a way by which the number of steps in a solution can be dramatically reduced. It also offers the mathematician a way of learning quickly whether a problem has a solution or not, without having to complete the entire immense computation that may be required.

According to the American journal *Science*, the discovery was first reported last January in the Soviet journal *Doklady*. It escaped notice in the West, however, partly because the article was in Russian and partly because its author, a graduate student, was unknown to mathematicians.

Proper attention was finally focused on the Russian paper by Dr. Eugene Lawler of the University of California at Berkeley. In the months since then, two mathematicians working at Stanford University, László Lovász of the University of Szeged in Hungary and Peter Gacs of the University of Rochester, have analyzed it in a paper of their own. Dr. Dantzig said that in the last few days the university was inundated by requests for the paper.

The Russian discovery proposes an approach for using computers to solve

a kind of problem related to the "Traveling Salesman Problem," one of the most famous and intractable in mathematics.

The object of the problem is to determine the shortest possible route a salesman must follow to visit any number of cities without returning to any city already visited. On its face, the problem seems simple, and in fact, computers routinely provide working answers to practical applications of the problem.

But with existing mathematical approaches, it is always possible to devise such problems for which there are no solutions.

The theoretical distinction between very hard and impossible is an important one in mathematics, and it can have far-reaching consequences in such practical applications as the devising of secret codes.

Protection of Computer Data

Several years ago, a major scientific and governmental controversy ensued following a proposal by a group of computer experts that the privacy of computer data be protected by coding according to a system related to the Traveling Salesman Problem.

The proposal was based on the idea that it is believed to be practically impossible to factor large numbers, in which the factors are prime numbers. A prime number, such as 3, 57, 7, or 11, is one that can be evenly divided only by itself and the number 1, not by any other whole number. To factor a number is to break the number down into smaller quantities, which when multiplied by each other, will recreate the original number. For example, factors of the number 12 could be 2 and 6 or 3 and 4 or 2 and 3.

If it could be shown that a secret code based on the factoring of large numbers into primes could be solved by a computer in a reasonable length of time, this method of encoding would presumably be made less secure. The theory of codes could eventually be affected by the Russian discovery, and this fact has obvious importance to intelligence organizations everywhere. No government is believed to be using such a code now.

Several American mathematicians expressed surprise at the seeming simplicity of the proposal by Mr. Khachiyan for solving the hard programs known as linear programming problems.

Vital Lesson Is Learned

"There is an important lesson in this," according to one of America's leading computer experts, Dr. Ronald L. Graham of Bell Laboratories, Holmdel, N.J. "You shouldn't assume that something is hard just because you can't do it. There may be some easy solution right in front of your nose that you keep missing."

Linear programming problems can seem very hard indeed.

Typically, a problem might involve the purchase of various foods at a market, with the idea that the nutritional ingredients in all of them meet a person's minimum daily requirement for the least cost. The problem involves many variables and "constraints," such as a maximum price stipulated for carrots.

There are many problems in which a large number of variables and constraints results in such complexity that a powerful computer would take billions of years to solve them using conventional methods. Furthermore, a mathematician cannot always tell in advance whether the problem is even theoretically solvable. The new Soviet approach can tell a computer operator quickly whether a solution exists. If so, a solution is guaranteed.

"Simplex Algorithm"

One approach that has been in use for years is called the "simplex algorithm" invented by Dr. Dantzig.

In the simplex method, a computer is programmed to "visualize" a polyhedral, or many faced, shape in space, in which each vertex, a point where three or more faces come together, represents one possible solution to the problem. The idea is to maneuver the computer into selecting the one vertex that represents the best answer—maximum, minimum, or whatever other quality the operator is seeking.

If a method based on the Soviet discovery were applied to this kind of problem, the basic shape "visualized" by the computer would be a curved ellipsoid rather than a flat-sided polyhedron, and the best solution would be represented by the smallest ellipsoid the computer could devise that would envelope the solution while fitting into the space allotted to it.

A computer must examine the vertices of a polyhedron one by one as it looks for the vertex representing the solution, but by considering ellipsoids, the computer can look at a larger part of the problem at one time, theoretically whittling the problem down more quickly.

"As far as we know, no one has yet put Khachiyan's idea to use in an actual computer program," Dr. Graham said, "but a period of active experimentation is beginning."

Among the government organizations that have shown strong interest, he said, is the National Center for Atmospheric Research. The problems in understanding the mechanics of weather and climate are so complex that many are currently insoluble by computer in any time less than billions of centuries of computation.

November 7, 1979

The Health Care Debate: Finding What Works

By GINA KOLATA

Buried in bulging files and stored in computers in doctors' offices, drug stores, insurance companies and hospitals is information on nearly everything that the health care profession has done to or prescribed for Americans in recent years. To some, the records are a gold mine. To others, they are a minefield.

But one thing is certain: the material is being unearthed. Insurers, drug companies and large health maintenance organizations are mounting an extensive effort to use medical data to decide which treatments are best, which doctors are best and which health plans keep people healthiest.

It is virtually certain that if a national health insurance bill is passed by Congress this year, it will include provisions for this sort of research, which is broadly called outcomes research. And the federal Agency for Healthcare Policy and Research is already financing outcomes studies.

The idea is to search computer files for patient information to see what works and what does not. Information would be gathered from medical records, medical diagnoses, insurance forms and written prescriptions. Researchers could ask, for example, whether patients who took cholesterol-lowering drugs had fewer heart attacks than those with similar cholesterol levels who did not take the drugs.

They could also ask how one company's drug compared with another company's. In a variation called physician profiling, investigators could analyze medical records to find doctors who used outdated treatments and those whose patients fared worse than average.

"A new cottage industry is emerging," said Robert Merold, a vice president at IMS America, a company in Totowa, N.J., that gathers data on drugs and medical care. "Everybody's scrambling."

Mr. Merold said drug companies and health maintenance organizations in particular were convinced that outcomes research would help them to prove to customers that their drugs and medical treatments are worth the money. "That's the best way to sell new products," Mr. Merold said.

It is also central to plans to change the health insurance system and make

people informed consumers, allowing them to choose the health care plans that give the best results at the lowest cost.

But critics say the only trustworthy way to learn what works in medicine is to allocate people at random to different treatments or health plans, monitor them from beginning to end and then assess the results. They say the data from medical records, insurance claims forms and pharmacy records are severely biased and therefore all but unusable. For example, one doctor may select the healthiest heart patients for surgery and treat the others with medications. If the surgical patients do better, that may be because they were healthier to begin with.

As a result, the critics say, it can be medically dangerous to treat the conclusions of this kind of outcomes research as scientific fact.

Outcomes research is complete rubbish, said Dr. Richard Peto, a statistics professor at Oxford University. "It's a bit like the emperor's new clothes," he said. "People think they have tons of data and so they must be able to analyze it to see what works. They say they'll use statistics" to make adjustments for biases and incompleteness.

Statisticians Object

"I've spent more than 20 years working as a statistician and I've got a silver medal from the Royal Society, and I can assure you that you cannot use statistics to adjust," Dr. Peto said.

But despite the alarms sounded by statisticians like Dr. Peto, companies and academic researchers are forging ahead.

For example, the Prudential Insurance Company of America has invested \$20 million in a new center to do outcomes research. It is directed by Dr. William Roper, the former head of the Health Care Financing Administration and of the Centers for Disease Control and Prevention.

Dr. Roper said he intended to use Prudential's data to decide what medical practices work and which doctors and health maintenance organizations in Prudential's network are most effective. "The people Prudential does business with, like Xerox, A.T.&T. and Delta Airlines, are pressing us for detailed information on how we're doing," he said. "They are no longer content for us to say that we process claims quickly and their employees are satisfied. They want to know, Are their employees healthier?"

Volumes of Information

Merck & Company, the drug manufacturer, is going to do its own outcomes research using data from Medco, a company it bought that manages prescription benefits for 38 million Americans. Medco has enormous amounts of data showing which doctors wrote which prescriptions for which patients and how often the prescriptions were refilled. Merck says it will use those files to determine which drugs are most effective.

John Doorley, a Merck spokesman, said that with the Medco files, "Merck can very quickly accumulate data on how patients are taking medications and what it means in terms of long-term and short-term clinical effects."

Health maintenance organizations are using the data to keep tabs on doctors. Dr. Keith Collins, vice president for medical support at Healthsource Inc., an H.M.O. based in Hooksett, N.H., that has 850,000 members in 12 states, said the company used profiling to pick out doctors who use too many, or too few, medical resources. Each quarter it shows doctors how they are doing compared with the average and punishes poor performers by withholding a percentage of their income or, in extreme cases, banishing them from Healthsource.

Academic investigators are publicly plumbing available data. For example, Dr. H. Gilbert Welsh of the Veterans Affairs Medical Center in White River Junction, Vt., and his colleagues recently published an analysis of Medicare claims data in *The New England Journal of Medicine* showing how doctors' practices in Florida and Oregon compare. The doctors in Florida, the investigators concluded, saw patients more often, admitted them to the hospital more frequently and did more medical tests and procedures than those in Oregon.

For the Sake of Debate

The researchers wrote that they did their analysis "in an effort to encourage further debate," and said profiling could be used to discover areas where medical services are overused, for example. Their article was accompanied by an editorial by Dr. Jerome P. Kassirer, the journal's editor, saying that physician profiling is a potentially useful tool but that no method has so far been without flaws.

Critics, however, are leery about claims that the flaws can ever be eliminated from the analyses. To take one example, they say, a patient's insurance claim form, like a Medicare form or one sent to a large insurer like Prudential, can reveal

more about the peculiarities of the health care reimbursement system than about the patient's illness.

Dr. John Wasson, director of the Center for Aging at Dartmouth College in Hanover, N.H., says doctors often "unbundle" their diagnoses, listing as many separate conditions as possible for insurance purposes. They also "upcode," diagnosing a more severe condition than the patient has, or they record fictitious medical problems on claim forms so that healthy people who come in for routine checkups will have their visits paid for by their insurance companies.

For example, Dr. Wasson said, the PSA, a popular prostate cancer screening test, is not covered by Medicare unless it is used to follow the progress of someone who already had cancer. So, he said, many doctors write in their records and on insurance claim forms that they are doing the test because a man has prostate cancer, even when he is perfectly healthy.

Truth Often Shrouded

Dr. Wasson said he would rarely trust medical records. "If the record says a guy had a hernia operation, he's generally had a hernia operation," he said. "But when you get to bronchitis versus pneumonia, good luck."

Dr. Alan L. Hillman, who directs the Center for Health Policy at the University of Pennsylvania, said medical records were hopelessly inadequate for studying medical practices. "You cannot do good outcomes research or cost-effectiveness research without knowing what actually happened to the patients," he said. "When data bases are designed to collect billing data or administrative data or anything else, they are used in that fashion and manipulated in that fashion. It is impossible to judge the outcomes of a clinical interaction on the basis of paperwork that is done now."

Dr. Roper said Prudential was well aware of that problem and hoped to correct it. Doctors would be instructed to enter true medical records into the company's special files to be used for outcomes research. It is, in effect, an attempt to create a second set of books.

But, even so, data can be muddled because patients are not allocated to different treatments at random. Treatments may differ between sicker patients and healthier ones, and between younger patients and older ones. Healthier people may gravitate toward one doctor or medical plan while sicker people seek out other doctors or plans.

Dr. Carl Morris, the chairman of the statistics department at Harvard University, says that with careful statistical analyses, these biases can be accounted for. It is not easy, he said, and he finds that the methods that most researchers use are flawed.

"What worries me is that things will get institutionalized before the best statistical methods are set up," he said. "There's a tendency to gravitate toward simple methods."

But Dr. Hillman said, "My biggest concern is that all data are not information, and just because you have a few pieces of data does not mean you can make decisions."

August 9, 1994

Step 1: Post Elusive Proof. Step 2: Watch Fireworks.

By JOHN MARKOFF

The potential of Internet-based collaboration was vividly demonstrated this month when complexity theorists used blogs and wikis to pounce on a claimed proof for one of the most profound and difficult problems facing mathematicians and computer scientists.

Vinay Deolalikar, a mathematician and electrical engineer at Hewlett-Packard, posted a proposed proof of what is known as the “P versus NP” problem on a Web site, and quietly notified a number of the key researchers in a field of study that focuses on problems that are solvable only with the application of immense amounts of computing power.

The researcher asserted that he had demonstrated that P (the set of problems that can be easily solved) does not equal NP (those problems for which solutions can be verified relatively quickly). As with earlier grand math challenges—for example, Fermat’s Last Theorem—there is a lot at stake, not the least of which is a \$1 million prize.

In 2000 the Clay Mathematics Institute picked seven of the greatest unsolved problems in the field, named them “Millennium Problems” and offered \$1 million for the solution of each of them. P versus NP is one of those problems. (In March, the first prize was awarded to a reclusive Russian mathematician, Grigori Perelman, for the solution to the century-old Poincaré conjecture. A few months later he refused the prize.)

P versus NP has enormous practical and economic importance, because modern cryptography is based on the assumption, which is workable so far, that P does not equal NP. In other words, there are problems that are impossible for computers to solve, but for which the solutions are easily recognizable. If these problems were shown to be solvable, that could undermine modern cryptography, which could paralyze electronic commerce and digital privacy because transactions would no longer be secure.

In a note sent to a small group of researchers on Aug. 6, Dr. Deolalikar wrote: “The proof required the piecing together of principles from multiple areas within mathematics. The major effort in constructing this proof was uncovering a chain of conceptual links between various fields and viewing them through a common lens.”

An outsider to the insular field, Dr. Deolalikar set off shock waves because his work appeared to be a concerted and substantial challenge to a problem that has attracted intense scrutiny since it was first posed in 1971 by Stephen Cook, a mathematician and computer scientist who teaches at the University of Toronto.

"The reason there was such excitement is there have been many alleged proofs," said Moshe Vardi, a professor of computer science at Rice University and the editor in chief of *Communications of the Association for Computing Machinery*. "This looks like a serious paper. In particular what he has done is bring forward a new idea that is worth exploring."

In this case, however, the significant breakthrough may not be in the science, but rather in the way science is practiced. By the middle of last week, although Dr. Deolalikar had not backed away from his claim, a consensus had emerged among complexity theorists that the proposed proof had several significant shortcomings.

"At this point the consensus is that there are large holes in the alleged proof—in fact, large enough that people do not consider the alleged proof to be a proof," Dr. Vardi said. "I think Deolalikar got his 15 minutes of fame, but at this point the excitement has subsided and the skepticism is turning into negative conviction."

What was highly significant, however, was the pace of discussion and analysis, carried out in real time on blogs and a wiki that had been quickly set up for the purpose of collectively analyzing the paper. This kind of collaboration has emerged only in recent years in the math and computer science communities. In the past, intense discussions like the one that surrounded the proof of the Poincaré conjecture were carried about via private e-mail and distribution lists as well as in the pages of traditional paper-based science journals.

Several of the researchers said that until now such proofs had been hashed out in colloquiums that required participants to be physically present at an appointed time. Now, with the emergence of Web-connected software programs it is possible for such collaborative undertakings to harness the brainpower of the world's best thinkers on a continuous basis.

In his recently published book *Cognitive Surplus: Creativity and Generosity in a Connected Age* (Penguin Press), Clay Shirky, a professor of interactive telecommunications at New York University, argues that the emergence of these new collaborative tools is paving the way for a second scientific revolution in the same way the printing press created a demarcation between the age of alchemy and the age of chemistry.

"The difference between the alchemists and the chemists was that the printing press was used to coordinate peer review," he said. "The printing press didn't cause the scientific revolution, but it wouldn't have been possible without it."

Now, he says, the new tools are likely to set off a similar transformation.

"It's not just, 'Hey, everybody, look at this,'" he said, "but rather a new set of norms is emerging about what it means to do mathematics, assuming coordinated participation."

The computer science community has long been an innovator in the design of science-collaboration tools. Indeed, the ARPAnet, the forerunner of the Internet, was initially created in 1969 to make one of the first computerized collaboration tools, Douglas Engelbart's oNLine System, or NLS, available from remote locations. During the 1980s physicists at the physics research center CERN near Geneva created the World Wide Web to facilitate the sharing of scientific research.

In 2009, a Cambridge mathematician, Timothy Gowers, created the Polymath Project, a blog and wiki-oriented collaboration tool that used the comments section of a blog to pursue mathematics collaboratively. Related efforts like the Web site Mathoverflow help attack unsolved mathematical problems by using new Internet tools to help stimulate collaboration.

In the case of the P versus NP paper, most of the action has taken place in several blogs maintained by researchers in the field, like a computer scientist, Richard Lipton, at Georgia Tech and a theoretical physicist, Dave Bacon, at the University of Washington, as well as in a wiki by a quantum theoretician, Michael Nielsen.

Passions have run high. A computer scientist at the Massachusetts Institute of Technology, Scott Aaronson, literally bet his house last week—\$200,000—that the Deolalikar paper would be proved incorrect: "If Vinay Deolalikar is awarded the \$1,000,000 Clay Millennium Prize for his proof of P-NP, then I, Scott Aaronson, will personally supplement his prize by the amount of \$200,000."

Despite his skepticism, he acknowledged that this was, to date, one of the most impressive attempts to settle the question.

"So far this is not your typical P versus NP crank solution, which I hear about once a week," he said.

August 16, 2010



CHAPTER 7

Mathematicians and Their World

SOME ARE LONERS, SOME ARE ICONOCLASTS, AND SOME ARE gregarious self-promoters. There is just one feature that defines great mathematicians—an inborn genius, a talent like that of an elite athlete or a gifted musician or exceptional artist. The profiles in this section show the range of mathematicians' talents and why these astonishingly creative people chose their field.

They include the rural uneducated Indian genius Srinivasa Ramanujan, who died at age 32 at the turn of the 20th century. Somehow, he intuited deep mathematical truths.

James Gleick, writing about Ramanujan, quotes a mathematician who says, "He seems to have functioned in a way unlike anybody else we know of. He had such a feel for things that they just flowed out of his brain."

Then there is Andrew Wiles, who solved the notorious Fermat's Last Theorem while working in seclusion for seven years in his attic office in his Princeton home. "No computer was necessary, and no telephone was present to intrude on the absolute silence," I wrote. He told no one what he was doing. One of his colleagues explained why: "If he said he was working on Fermat's Last Theorem, people would look

askance. And if you start telling people who are experts, you end up collaborating with them. He wanted to do it on his own."

John Horton Conway, one of Wiles's colleagues at Princeton, loves games and puzzles and wants to learn odd facts, like the digits of π extended to 1,000 places or the name and location of every visible star.

He became famous in 1969, when he was working at the University of Cambridge, desperately seeking recognition, and took up a hard problem.

"Basically, I said goodbye to my wife, kissed the kids and stuck myself in the front room." To his own amazement, he solved the problem in 12 hours.

The list, and the stories, go on, each personality offering a different view into the world of mathematics and why it drew each of them. The chapter ends with an article by George Johnson on one other type of personality drawn to the field. Mathematicians call them the math cranks.

And they pose a dilemma as they send out lengthy missives to well-known mathematicians, demanding a hearing, someone to look over what they say is pathbreaking work.

"Who is going to stroll through pages and pages of stuff that is very hard to understand when you don't have to do it?" one mathematician told Johnson. "From the point of view of these guys, we are arrogant, unwilling to reconsider ideas. And why shouldn't they expect a responsible scientist to look carefully at some new idea that might be important?"

"You can't just say Ramanujan was a genius and these other guys were cranks. With a superficial look, there is hardly any visible difference. There is not always a sharp line between eccentric mathematicians and intelligent but maybe obsessed amateurs."

Paul Erdos, 83, a Wayfarer in Math's Vanguard, Is Dead

By GINA KOLATA

Paul Erdos, a legendary mathematician who was so devoted to his subject that he lived as a mathematical pilgrim with no home and no job, died on Friday in Warsaw. He was 83.

The cause of death was a heart attack, according to an e-mail message sent out this weekend by Dr. Miki Simonovits, a mathematician at the Hungarian Academy of Sciences, who was a close friend.

Dr. Erdos (pronounced AIR-dosh) was attending a mathematics meeting in Warsaw when he died, Dr. Simonovits reported.

The news, only now reaching the world's mathematicians, has come as a blow. Dr. Ronald L. Graham, the director of the information sciences research center at A.T.&T. Laboratories, said, "I'm getting e-mail messages from around the world, saying, 'Tell me it isn't so.'"

Never, mathematicians say, has there been an individual like Paul Erdos. He was one of the century's greatest mathematicians, who posed and solved thorny problems in number theory and other areas and founded the field of discrete mathematics, which is the foundation of computer science. He was also one of the most prolific mathematicians in history, with more than 1,500 papers to his name. And, his friends say, he was also one of the most unusual.

Dr. Erdos "is on the short list for our century," said Dr. Joel H. Spencer, a mathematician at New York University's Courant Institute of Mathematical Sciences.

Dr. Graham said, "He's among the top 10."

Dr. Ernst Straus, who worked with both Albert Einstein and Dr. Erdos, wrote a tribute to Dr. Erdos shortly before his own death in 1983. He said of Dr. Erdos: "In our century, in which mathematics is so strongly dominated by 'theory doctors,' he has remained the prince of problem solvers and the absolute monarch of problem posers." Dr. Erdos, he continued, is "the Euler of our time," referring to the great 18th-century mathematician, Leonhard Euler, whose name is spoken with awe in mathematical circles.

Stooped and slight, often wearing socks and sandals, Dr. Erdos stripped himself of all the quotidian burdens of daily life: finding a place to live, driving

a car, paying income taxes, buying groceries, writing checks. "Property is nuisance," he said.

Concentrating fully on mathematics, Dr. Erdos traveled from meeting to meeting, carrying a half-empty suitcase and staying with mathematicians wherever he went. His colleagues took care of him, lending him money, feeding him, buying him clothes and even doing his taxes. In return, he showered them with ideas and challenges—with problems to be solved and brilliant ways of attacking them.

Dr. László Babai of the University of Chicago, in a tribute written to celebrate Dr. Erdos's 80th birthday, said Dr. Erdos's friends "care for him fondly, repaying in small ways for the light he brings into their homes and offices."

Mathematicians like to brag about their connections to Dr. Erdos by citing their "Erdos number." A person's Erdos number is 1 if he or she has published a paper with Dr. Erdos. It is 2 if he or she has published with someone who has published with Erdos, and so on. At last count, Dr. Erdos had 458 collaborators, Dr. Graham said. An additional 4,500 mathematicians had an Erdos number of 2, Dr. Graham added. He said so many mathematicians were still at work on problems they had begun with Dr. Erdos that another 50 to 100 papers with Dr. Erdos's name on them were expected to be published after his death.

Dr. Graham, whose Erdos number is 1, handled Dr. Erdos's money for him, setting aside an "Erdos room" in his house for the chore. He said Dr. Erdos had given away most of the money he earned from lecturing at mathematics conferences, donating it to help students or as prizes for solving problems he had posed. Dr. Erdos left behind only \$25,000 when he died, Dr. Graham said, and he plans to confer with other mathematicians about how to give it away to help mathematics.

Dr. Graham said Dr. Erdos's "driving force was his desire to understand and to know." He added, "You could think of it as Erdos's magnificent obsession. It determined everything in his life."

Dr. Spencer, of New York University, who also has an Erdos number of 1, said, "He was always searching for mathematical truths." He added: "Erdos had an ability to inspire. He would take people who already had talent, that already had some success, and just take them to an entirely new level. His world of mathematics became the world we all entered."

Born in Hungary in 1913, Dr. Erdos was a cosseted mathematical prodigy. At age 3, Dr. Graham said, Dr. Erdos discovered negative numbers for himself when

he subtracted 250 degrees from 100 degrees and came up with 150 degrees below zero. A few years later, he amused himself by solving problems he had invented, like how long would it take for a train to travel to the sun.

Dr. Erdos had two older sisters who died of scarlet fever a few days before he was born, so his mother became very protective of him. His parents, who were mathematics teachers, took him out of public school after just a few years, Dr. Graham said, and taught him at home with the help of a German governess. And, Dr. Graham said, Dr. Erdos's mother coddled him. "Erdos had never buttered his own toast until he was 21 years old," Dr. Graham said. He never married and left no immediate survivors.

When Dr. Erdos was 20, he made his mark as a mathematician, discovering an elegant proof for a famous theorem in number theory. The theorem, Chebyshev's theorem, says that for each number greater than 1, there is always at least one prime number between it and its double. A prime number is one that has no divisors other than itself and 1.

Although his research spanned a variety of areas of mathematics, Dr. Erdos kept up his interest in number theory for the rest of his life, posing and solving problems that were often simple to state but notoriously difficult to solve and that, like Chebyshev's theorem, involved relationships between numbers. "He liked to say that if you can state a problem in mathematics that's unsolved and over 100 years old, it is probably a problem in number theory," Dr. Graham said.

Dr. Erdos, like many mathematicians, believed that mathematical truths are discovered, not invented. And he had an evocative way of conveying that notion. He spoke of a Great Book in the sky, maintained by God, that contained the most elegant proofs of every mathematical problem. He used to joke about what he might find if he could just have a glimpse of that book.

He would also muse about the perfect death. It would occur just after a lecture, when he had just finished presenting a proof and a cantankerous member of the audience would have raised a hand to ask, "What about the general case?" In response, Dr. Erdos used to say, he would reply, "I think I'll leave that to the next generation," and fall over dead.

Dr. Erdos did not quite achieve his vision of the perfect death, Dr. Graham said, but he came close.

"He died with his boots on, in hand-to-hand combat with one more problem," Dr. Graham said. "It was the way he wanted to go."

September 24, 1996

Journeys to the Distant Fields of Prime

By KENNETH CHANG



Four hundred people packed into an auditorium at U.C.L.A. in January to listen to a public lecture on prime numbers, one of the rare occasions that the topic has drawn a standing-room-only audience.

Another 35 people watched on a video screen in a classroom next door. Eighty people were turned away.

The speaker, Terence Tao, a professor of mathematics at the university, promised "a whirlwind tour, the equivalent to going through Paris and just seeing the Eiffel Tower and the Arc de Triomphe."

His words were polite, unassuming and tinged with the accent of Australia, his homeland. Even though prime numbers have been studied for 2,000 years, "There's still a lot that needs to be done," Dr. Tao said. "And it's still a very exciting field."

After Dr. Tao finished his one-hour talk, which was broadcast live on the Internet, several students came down to the front and asked for autographs.

Dr. Tao has drawn attention and curiosity throughout his life for his prodigious abilities. By age 2, he had learned to read. At 9, he attended college math classes. At 20, he finished his Ph.D.

Now 31, he has grown from prodigy to one of the world's top mathematicians, tackling an unusually broad range of problems, including ones involving prime numbers and the compression of images. Last summer, he won a Fields Medal, often considered the Nobel Prize of mathematics, and a MacArthur Fellowship, the "genius" award that comes with a half-million dollars and no strings.

"He's wonderful," said Charles Fefferman of Princeton University, himself a former child prodigy and a Fields Medalist. "He's as good as they come. There are a few in a generation, and he's one of the few."

Colleagues have teasingly called Dr. Tao a rock star and the Mozart of Math. Two museums in Australia have requested his photograph for their permanent exhibits. And he was a finalist for the 2007 Australian of the Year award.

"You start getting famous for being famous," Dr. Tao said. "The Paris Hilton effect."

Not that any of that has noticeably affected him. His campus office is adorned with a poster of *Ranma ½*, a Japanese comic book series. As he walks the halls of the math building, he might be wearing an Adidas sweatshirt, blue jeans and scruffy sneakers, looking much like one of his graduate students. He said he did not know how he would spend the MacArthur money, though he mentioned the mortgage on the house that he and his wife, Laura, an engineer at the NASA Jet Propulsion Laboratory, bought last year.

After a childhood in Adelaide, Australia, and graduate school at Princeton, Dr. Tao has settled into sunny Southern California.

"I love it a lot," he said. But not necessarily for what the area offers.

"It's sort of the absence of things I like," he said. No snow to shovel, for instance.

A deluge of media attention following his Fields Medal last summer has slowed to a trickle, and Dr. Tao said he was happy that his fame might be fleeting so that he could again concentrate on math.

One area of his research—compressed sensing—could have real-world use. Digital cameras use millions of sensors to record an image, and then a computer chip in the camera compresses the data.

"Compressed sensing is a different strategy," Dr. Tao said. "You also compress the data, but you try to do it in a very dumb way, one that doesn't require much computer power at the sensor end."

With Emmanuel Candès, a professor of applied and computational mathematics at the California Institute of Technology, Dr. Tao showed that even if most of the information were immediately discarded, the use of powerful algorithms could still reconstruct the original image.

By useful coincidence, Dr. Tao's son, William, and Dr. Candès's son attended the same preschool, so dropping off their children turned into useful work time.

"We'd meet each other every morning at preschool," Dr. Tao said, "and we'd catch up on what we had done."

The military is interested in using the work for reconnaissance: blanket a battlefield with simple, cheap cameras that might each record a single pixel of data. Each camera would transmit the data to a central computer that, using the mathematical technique developed by Dr. Tao and Dr. Candès, would construct a comprehensive view. Engineers at Rice University have made a prototype of just such a camera.

Dr. Tao's best-known mathematical work involves prime numbers—positive whole numbers that can be divided evenly only by themselves and 1. The first few prime numbers are 2, 3, 5, 7, 11 and 13 (1 is excluded).

As numbers get larger, prime numbers become sparser, but the Greek mathematician Euclid proved sometime around 300 B.C. that there is nonetheless an infinite number of primes.

Many questions about prime numbers continue to elude answers. Euclid also believed that there was an infinite number of "twin primes"—pairs of prime numbers separated by 2, like 3 and 5 or 11 and 13—but he was unable to prove his conjecture. Nor has anyone else in the succeeding 2,300 years.

A larger unknown question is whether hidden patterns exist in the sequence of prime numbers or whether they appear randomly.

In 2004, Dr. Tao, along with Ben Green, a mathematician now at the University of Cambridge in England, solved a problem related to the Twin Prime Conjecture by looking at prime number progressions—series of numbers equally spaced. (For example, 3, 7 and 11 constitute a progression of prime numbers with a spacing of 4; the next number in the sequence, 15, is not prime.) Dr. Tao and Dr. Green proved that it is always possible to find, somewhere in the infinity of integers, a progression of any length of equally spaced prime numbers.

"Terry has a style that very few have," Dr. Fefferman said. "When he solves the problem, you think to yourself, 'This is so obvious and why didn't I see it? Why didn't the 100 distinguished people who thought about this before not think of it?'"

Dr. Tao's proficiency with numbers appeared at a very young age. "I always liked numbers," he said.

A 2-year-old Terry Tao used toy blocks to show older children how to count. He was quick with language and used the blocks to spell words like "dog" and "cat."

"He probably was quietly learning these things from watching *Sesame Street*," said his father, Dr. Billy Tao, a pediatrician who immigrated to Australia from Hong Kong in 1972. "We basically used *Sesame Street* as a babysitter."

The blocks had been bought as toys, not learning tools. "You expect them to throw them around," said the elder Dr. Tao, whose accent swings between Australian and Chinese.

Terry's parents placed him in a private school when he was 3½. They pulled him out six weeks later because he was not ready to spend that much time in a classroom, and the teacher was not ready to teach someone like him.

At age 5, he was enrolled in a public school, and his parents, administrators and teachers set up an individualized program for him. He proceeded through each subject at his own pace, quickly accelerating through several grades in math and science while remaining closer to his age group in other subjects. In English classes, for instance, he became flustered when he had to write essays.

"I never really got the hang of that," he said. "These very vague, undefined questions. I always liked situations where there were very clear rules of what to do."

Assigned to write a story about what was going on at home, Terry went from room to room and made detailed lists of the contents.

When he was $7\frac{1}{2}$, he began attending math classes at the local high school.

Billy Tao knew the trajectories of child prodigies like Jay Luo, who graduated with a mathematics degree from Boise State University in 1982 at the age of 12, but who has since vanished from the world of mathematics.

"I initially thought Terry would be just like one of them, to graduate as early as possible," he said. But after talking to experts on education for gifted children, he changed his mind.

"To get a degree at a young age, to be a record-breaker, means nothing," he said. "I had a pyramid model of knowledge, that is, a very broad base and then the pyramid can go higher. If you just very quickly move up like a column, then you're more likely to wobble at the top and then collapse."

Billy Tao also arranged for math professors to mentor Terry.

A couple of years later, Terry was taking university-level math and physics classes. He excelled in international math competitions. His parents decided not to push him into college full time, so he split his time between high school and Flinders University, the local university in Adelaide. He finally enrolled as a full-time college student at Flinders when he was 14, two years after he would have graduated had his parents pushed him only according to his academic abilities.

The Taos had different challenges in raising their other two sons, although all three excelled in math. Trevor, two years younger than Terry, is autistic with top-level chess skills and the musical savant gift to play back on the piano a musical piece—even one played by an entire orchestra—after hearing it just once. He completed a Ph.D. in mathematics and now works for the Defence Science and Technology Organisation in Australia.

The youngest, Nigel, told his father that he was "not another Terry," and his parents let him learn at a less accelerated pace. Nigel, with degrees in economics,

math and computer science, now works as a computer engineer for Google Australia.

"All along, we tend to emphasize the joy of learning," Billy Tao said. "The fun is doing something, not winning something."

Terry completed his undergraduate degree in two years, earned a master's degree a year after that, then moved to Princeton for his doctoral studies. While he said he never felt out of place in a class of much older students, Princeton was where he finally felt he fit among a group of peers. He was still younger, but was not necessarily the brightest student all the time.

His attitude toward math also matured. Until then, math had been competitions, problem sets, exams. "That's more like a sprint," he said.

Dr. Tao recalled that as a child, "I remember having this vague idea that what mathematicians did was that, some authority, someone gave them problems to solve and they just sort of solved them."

In the real academic world, "Math research is more like a marathon," he said.

As a parent and a professor, Dr. Tao now has to think about how to teach math in addition to learning it.

An evening snack provided him an opportunity to question his son, who is 4. If there are 10 cookies, how many does each of the five people in the living room get?

William asked his father to tell him. "I don't know how many," Dr. Tao replied. "You tell me."

With a little more prodding, William divided the cookies into five stacks of two each.

Dr. Tao said a future project would be to try to teach more non-mathematicians how to think mathematically—a skill that would be useful in everyday tasks like comparing mortgages.

"I believe you can teach this to almost anybody," he said.

But for now, his research is where his focus is.

"In many ways, my work is my hobby," he said. "I always wanted to learn another language, but that's not going to happen for a while. Those things can wait."

March 13, 2007

Highest Honor in Mathematics Is Refused

By KENNETH CHANG

Grigori Perelman, a reclusive Russian mathematician who solved a key piece in a century-old puzzle known as the Poincaré conjecture, was one of four mathematicians awarded the Fields Medal today.

But Dr. Perelman refused to accept the medal, as he has other honors, and he did not attend the ceremonies at the International Congress of Mathematicians in Madrid.

"I regret that Dr. Perelman has declined to accept the medal," Sir John M. Ball, president of the International Mathematical Union, said during the ceremonies.

The Fields Medal, often described as mathematics' equivalent to the Nobel Prize, is given every four years, and several can be awarded at once. Besides Dr. Perelman, three professors of mathematics were awarded Fields Medals this year: Andrei Okounkov of Princeton; Terence Tao of University of California, Los Angeles; and Wendelin Werner of the University of Paris-Sud in Orsay.

Dr. Perelman, 40, is known not only for his work on the Poincaré conjecture, among the most heralded unsolved math problems, but also because he has declined previous mathematical prizes and has turned down job offers from Princeton, Stanford and other universities. He has said he wants no part of \$1 million that the Clay Mathematics Institute in Cambridge, Mass. has offered for the first published proof of the conjecture.

In June, Dr. Ball traveled to St. Petersburg, Russia, where Dr. Perelman lives, for two days in hopes of persuading him to go to Madrid and accept the medal.

"He was very polite and cordial, and open and direct," Dr. Ball said in an interview.

But he was also adamant. "The reasons center around his feeling of isolation from the mathematical community," Dr. Ball said of Dr. Perelman's refusal, "and in consequence his not wanting to be a figurehead for it or wanting to represent it."

Dr. Ball added, "I don't think he meant it as an insult. He's a very polite person. There was never a cross word."

Despite Dr. Perelman's refusal, he is still officially a Fields Medalist. "He has a say whether he accepts it, but we have awarded it," Dr. Ball said.

Beginning in 2002, Dr. Perelman, then at the Steklov Institute of Mathematics of the Russian Academy of Sciences in St. Petersburg, published a series of papers on the Internet and gave lectures at several American universities describing how he had overcome a roadblock in the proof of the Poincaré conjecture.

The conjecture, devised by Henri Poincaré in 1904, essentially says that the only shape that has no holes and fits within a finite space is a sphere. That is certainly true looking at two-dimensional surfaces in the everyday three-dimensional world, but the conjecture says the same is true for three-dimensional surfaces embedded in four dimensions.

Dr. Perelman solved a difficult problem that other mathematicians had encountered when trying to prove the conjecture, using a technique called Ricci flow that smoothes out bumps in a surface and transforms it into a simpler form.

Dr. Okounkov, born in 1969 in Moscow, was recognized for work that tied together different fields of mathematics that had seemed unrelated. "This is the striking feature of Okounkov's work, finding unexpected links," said Enrico Arbarello, a professor of geometry at the University of Rome in Italy.

Dr. Okounkov's work has found use in describing the changing surfaces of melting crystals. The boundary between melted and non-melted is created randomly, but the random process inevitably produces a border in the shape of a heart.

Dr. Tao, a native of Australia and one of the youngest Fields Medal winners ever at age 31, has worked in several different fields, producing significant advances in the understanding of prime numbers, techniques that might lead to simplifying the equations of Einstein's theory of general relativity and the equations of quantum mechanics that describe how light bounces around in a fiber optic cable.

Dr. Werner, born in Germany in 1968, has also worked at the intersection of mathematics and physics, describing phenomena like percolation and shapes produced by the random paths of Brownian motion.

The medal was conceived by John Charles Fields, a Canadian mathematician, "in recognition of work already done and as an encouragement for further achievements on the part of the recipient."

Since 1936, when the medal was first awarded, judges have interpreted the terms of Dr. Fields's trust fund to mean that the award should usually be limited to mathematicians 40 years old or younger.

August 22, 2006

Scientist at Work: John H. Conway; At Home in the Elusive World of Mathematics

By GINA KOLATA

Dr. John H. Conway sits down at his computer and gets ready to log on. But before the computer allows him to begin work, it quickly spews out 10 randomly selected dates from the past and the future, dates like 3/15/2005 or 4/29/1803. Dr. Conway has to mentally calculate what day of the week each would be before his computer lets him open a file and get to work.

It is a game he has rigged up to play with himself. "I think I'm the fastest person in the world at this," he says. His record is 15.92 seconds to calculate all 10 days. But, he modestly says, it is not that hard. "It's the kind of thing autistic kids do."

Dr. Conway is unlike any other mathematician at Princeton University, and even in the field at large he stands out for the originality of his work on a mix of disparate and difficult subjects, including number theory, knot theory, the theory of quadratic forms and the theory of games.

And in a profession where quirky skills, like being a lightning calculator, are not unexpected, he is also remarkable for his odd and unusual interests and abilities. He is obsessed with games and puzzles, and has a thirst to learn unusual facts, like the digits of pi extended to 1,000 places or the name and location of every star in the heavens. "It took me a year to learn that," the 55-year-old mathematician said, explaining that the sky changes each night. But, at the same time, he has made significant mathematical discoveries of both theoretical and practical importance.

Dr. Ronald L. Graham, adjunct director for the information science division at A.T.&T. Bell Laboratories in Murray Hill, N.J., described Dr. Conway as "one of the most original mathematicians" around. "He's definitely world class, yet he has this kind of childlike enthusiasm," Dr. Graham said. "He's confident enough to work on any crazy thing he wants to." He added that Dr. Conway was entitled to veer off the beaten path. "He's certainly achieved enough," Dr. Graham said.

But Dr. Conway has so many peculiar interests and quirks, and he can so easily be made to sound eccentric, that his deep love of mathematics and the

natural world can be lost in the fluff. In a way, he is oblivious to the routines and customs of ordinary life. He recently bought a pair of shoes, after wearing only sandals, even in winter, since 1969. Three weeks ago, he went to a barber for the first time in 30 years—he had been wearing his hair in a ponytail and periodically hacking it off at the ends.

Yet though indifferent to fashion or fads, Dr. Conway is intensely aware of nature, and wants to know it deeply and intimately. He is infinitely curious and observant, seeing nature not only in a spider web or the details of a daffodil but in mathematics. Part of his way of getting to know the world is through an eclectic mixture of problems, ranging from the logic of quantum mechanics to the best way to pack eight-dimensional spheres, to devising an esthetically pleasing design for an artist who is going to plant a mountain with trees and wants to be sure that the design remains intact when trees are removed as the forest matures.

Dr. Conway was born and reared in Liverpool, England, the son of a laboratory assistant at the Liverpool Institute for Boys, a school that was attended by Paul McCartney and John Lennon of the Beatles. His talents in mathematics were always apparent. "My mother used to say she found me reciting the powers of 2 when I was 4 years old," he said. "I don't know if it's true and I don't know how far I got. It may be just one of those motherly stories." When he went to school, he said, "I was universally good at everything; I was the top or second or third in my class in every subject."

Yet mathematics always had a special appeal for Dr. Conway, and not just because he was good at calculations.

"This Other World"

"What turned me on was this mysterious relationship between things," he said. "There is this wonderful world of logic and connections that is very difficult to see. I can see trees and cats and people, but there is this other world and it's very, very powerful."

He explained that mathematical logic, the sort of reasoning that ties abstract ideas together, fascinated him and made him wonder how real it all was. Were abstract mathematical constructions illusions or reality? Were they a creation of the human mind or were they describing the essence of reality? Or, is mathematics discovered or invented?

Dr. Conway, along with many other mathematicians, believes that mathematics is discovered because, over and over again, abstract mathematical ideas, found purely by thought and reasoning, have turned out to provide exact descriptions of the physical world.

For example, he has been doing research with Dr. Neil Sloane of Bell Labs on sphere packing, which involves figuring the best way to pack spheres into a particular space. The work would seem to be an abstract and useless exercise. But it turns out that the eight-dimensional sphere packing problem is exactly what is needed to find the best way to transmit data, like the dimensions of a sound wave made by a human voice, along telephone lines. The idea is to take every eight data points, which name a point in eight-dimensional space, round them off, and transmit the rounded point. The rounded point is the center of the nearest eight-dimensional sphere.

Book on Sphere Packing

"I find it really lovely that this purely geometrical thing that I'm interested in is actually useful to quite practical people," Dr. Conway said.

Dr. Conway and Dr. Sloane recently wrote a book about their sphere packing work, which was reviewed in the journal *Advances in Mathematics* by Dr. Gian-Carlo Rota of the Massachusetts Institute of Technology.

It went, in part, like this: "This is the best survey of the best work in the best fields of combinatorics written by the best people. It will make the best reading by the best students interested in the best mathematics that is now going on." Dr. Conway calls it the "best" review.

Dr. Conway got his start as a renowned mathematician in 1969, when he was a faculty member at Cambridge University, hoping desperately to make a mark on the world. He was married and had four little girls. "I knew that I was a good mathematician, but the world didn't," he said. "I was getting very depressed because I hadn't lived up to the promise."

Another mathematician announced that he had discovered a new mathematical object, a highly symmetrical creation, in 24-dimensional space. By studying this, mathematicians hoped to find a new group, the concept they use to understand symmetry. But the discovery was preliminary and required working out the rules and symmetries to establish the group. Dr. Conway decided to make the attempt.

"I had this great plan," he recalled. "We were very poor at the time and I was doing lots of teaching to make ends meet. My plan was that I would work on it on Wednesday evenings from six until midnight and on Saturdays from 12 noon until midnight. I told my wife that this was very important."

Surprisingly Quick Solution

He started work on a Saturday. "It was very funny," he said. "Basically, I said goodbye to my wife, kissed the kids and stuck myself in the front room." Twelve and a half hours later he emerged, to his own astonishment, with the task completed.

That was the turning point in Dr. Conway's career. "It catapulted me into the jet set," he said. Soon he was traveling around the world, much in demand to describe his work. "I remember flying to New York to give a 20-minute lecture and then flying back again," he said.

The discovery "had a great psychological effect," Dr. Conway said. "It cured this depression and it also totally removed my ambition. I've been totally successful, but at some level I couldn't care less." He used to dream of being like most of his colleagues who "think of very deep things," he said. But with his momentous proof of the existence of what has come to be called the Conway Group, "that sort of removed that feeling." He added, "I decided that I might as well enjoy myself instead."

So what does he do to enjoy himself? For one, he indulges in his fascination with symmetries. He studies the petals of a daffodil, figuring out why there have to be an alternation of three true petals and three leaflike petals called setals. "I feel like I understand it," he said. "It gives me a nice feeling of being in tune with the world. It's a feeling of harmony."

A Deep Look at Pi

Or he decides to memorize the first 1,000 digits of pi. This was a project that his second wife, Dr. Larissa Conway, a Russian-born mathematician with whom Dr. Conway has two little boys, instigated when one day she needed the value of pi and knew it only as 3.14.

"I taught her the first 100 places, but she wanted more," Dr. Conway said. "I discovered I didn't know any more," he said, so he and his wife made it a project to

memorize 100 digits a day. The two would practice together during their regular routines.

"It was really rather sweet," Dr. Conway said. "We used to go on a walk on Sundays to the village and one person would recite 20 digits as we walked along, like a little poem, then hand it over to the next person and they would take over for the next 20 places."

He went on: "As I'm getting older, I'm finding that rather than having a deep understanding of lots and lots of problems, I like just knowing lots and lots of things.

"I don't mean facts—I mean things. Knowing what a daffodil looks like or the 633d digit of pi. Whatever it is. Some are show-offy. Most have no earthly use. I just like the feeling, and it is of some use to me professionally."

Asked how he actually does research, Dr. Conway describes a life of the mind that to most experimental scientists would seem unbearably frustrating. "What happens most of the time is nothing," he said. "You just can't have ideas often." When he does not know what to try to prove, he says, he will just start enumerating something. "I might try and list all the polyhedra with nice properties," he said. "With any luck, I'll see something."

It is a method that gets him through the dry days, he said and one that eludes most young researchers. "One of the terrible things that happen to bright young graduate students is they'll come in at 9 a.m. and write 'theorem' at the top of their paper. Then they might write 'proof.' Then they sit there staring at this thing. They get depressed, they go home at 5. They come in the next day and start again." The problem, he explained, is that "there's no way of proving a theorem to order. If someone comes up with a gun and says, 'Prove this theorem,' well, then, you're just dead."

Just an Ordinary Day

A typical day for Dr. Conway starts at about 8 a.m. when he goes to a local coffee shop and reads a newspaper over a breakfast of oatmeal. Then he turns on his computer, works out 10 dates and reads his e-mail. "There might be a math problem in the e-mail that might make me think," he explained. He will often have very long telephone conversations with Dr. Sloane about the work they are doing together or he might go to Bell Labs to work. He is teaching two classes this semester.

"The point is, I don't work," Dr. Conway said. "I mean, honestly, if you or your readers saw what I actually did, they'd be disgusted. They'd say, 'Good money is being paid out to support these people.'"

Dr. Conway said he used to feel guilty about the way he worked. "Then it suddenly dawned on me that that's the way I produce good stuff—by lying around, doing nothing, thinking about what I like," he said. And, he added, "I've been a lot more successful since I stopped feeling guilty."

October 12, 1993

Claude Shannon, B. 1916—Bit Player

By JAMES GLEICK

Halfway through the last century, information became a thing. It became a commodity, a force—a quantity to be measured and analyzed. It's what our world runs on. Information is the gold and the fuel. We measure it in bits. That's largely because of Claude Shannon.

Shannon is the father of information theory, an actual science devoted to messages and signals and communication and computing. The advent of information theory can be pretty well pinpointed: July 1948, the *Bell System Technical Journal*, his landmark paper titled simply "A Mathematical Theory of Communication." Before that, no such theory existed. Suddenly, there it was, almost full grown.

To treat information scientifically, engineers needed to answer the kinds of questions they were asking about matter and energy: How much? How fast? For fundamental particles, an irreducible unit of measure, Shannon proposed the word "bits"—as shorthand (suitably compressed) for "binary digits." A bit is a choice. On or off. Yes or no. One or zero. Shannon saw that these pairs are all the same. Information is fungible: smoke signals and semaphores, telegraph and television, all channels carrying bits.

Back then, the main technologies for sending and storing information were analog, not digital, so this was far from obvious. Phonograph records embodied sound waves in vinyl, and Shannon's telephone-company employers trafficked mostly in wavy signals, too. Yet some interesting communications channels were not continuous but discrete: the telegraph and teletype.

Mainly, though, Shannon was thinking of electrical circuits. The marriage of on-off to yes-no meant that circuits could carry out something akin to logic. They could not only transmit bits; they could manipulate them. Not coincidentally, in that same year Bell Labs was preparing to announce a new invention: the transistor. "It is almost certain," *Scientific American* declared bravely in 1952, "that 'bit' will become common parlance in the field of information, as 'horsepower' is in the motor field." Sure enough, bits led to bytes and, inexorably, to kilobytes, megabytes, gigabytes and terabytes.

All that still rests on the theoretical foundation laid by this playful mathematician and electrical engineer. Shannon was born in rural Michigan in 1916,

the son of a language teacher and a probate judge. He was an early and enthusiastic tinkerer in the new American style. Thomas Edison was his hero. Once he built a crude telegraph using a half-mile of barbed wire between his house and a friend's.

Nor did he stop playing just because he grew up. At Bell Labs, and then as a professor at the Massachusetts Institute of Technology, he amused colleagues by building juggling machines, unicycles, chess-playing computers and robotic turtles. He left a body of work comprising more than a hundred technical papers along the lines of "Reliable Circuits Using Less Reliable Relays," as well as others, not quite so influential, like "Scientific Aspects of Juggling" and "The Fourth-Dimensional Twist, or a Modest Proposal in Aid of the American Driver in England." He was also the author of "A Rubric on Rubik Cubics," which can be sung to the tune of "Ta-ra-ra-boom-de-ay."

When modern theorists worry about compressing data, maximizing bandwidth and coping with noise, they use the tools Shannon provided. They also keep in mind a paradox he emphasized from the very beginning—one that is either lovely or perverse, depending on your point of view. Information, in its new scientific sense, is utterly divorced from meaning. Chaotic systems, and strings of random numbers, altogether meaningless, are dense with information.

The medium, it turns out, is not the message. Words, sounds, pictures or gibberish—it's still just bits.

December 30, 2001

An Isolated Genius Is Given His Due

By JAMES GLEICK

In some ways, mathematicians are finally beginning to penetrate the mind of Srinivasa Ramanujan.

One hundred years have passed since Ramanujan was born in the small city of Kumbakonam in southern India. When he died 32 years later, he left a strange, raw legacy, about 4,000 formulas written on the pages of three notebooks and some scrap paper.

Some of the power and originality of Ramanujan's mathematics was understood a few years before his death. His contemporaries saw from the theorems scrawled across his pages that he possessed a genius for calculating the hidden laws and relationships that govern the wilderness of numbers.

But Ramanujan was uneducated in standard mathematics and isolated by geography for most of his productive life. Often his formulas seemed as obscure as they were elegant. He worked in a place of his own and a way of his own, drawing his formulas and theorems from a mental landscape that remained far from the frontier of mathematics as it was seen in his day.

Now his work is flowing into mathematics and science more deeply than could have been imagined a generation ago. Computers, with special programs to manipulate algebraic quantities, have made it possible for more ordinary mathematicians to pick up the trail of his thought. And modern physics, from the superstring theory of cosmology to the statistical mechanics of complicated molecular systems, finds itself turning more and more often to the pure findings of number theory and complex analysis—the worlds of Ramanujan.

So researchers are intensifying a process of forensic mathematics, or mathematical archeology—poring over the rough pages, trying to understand the formulas and prove them. As they learn more of why Ramanujan chose particular paths, they sense a foundation that has not yet been revealed.

"When he pulled extraordinary objects out of the air, they weren't just curiosities but they were the right things," said Jonathan M. Borwein of Dalhousie University in Halifax, Nova Scotia, one of many mathematicians who has lately found himself turning to Ramanujan's formulas. "They are elusive evidence of a theory that's lurking around somewhere that he never made explicit."

The trail is hard to follow. Out of necessity and then perhaps out of habit,

Ramanujan worked in a style that awes and frustrates modern mathematicians. He used a slate, jotting down formulas, erasing them with his elbow, jotting down more, and then recording a result in his precious notebook only when it had reached final form.

The intermediate results, the links of the chain, are lost. Unlike mainstream mathematicians, he felt no need to prove that a result was true. His legacy is simply a set of discoveries.

“A Feel for Things”

“He seems to have functioned in a way unlike anybody else we know of,” Dr. Borwein said. “He had such a feel for things that they just flowed out of his brain. Perhaps he didn’t see them in any way that’s translatable. It’s like watching somebody at a feast you haven’t been invited to.”

So mathematicians have spent years—often valuable and productive years—proving theorems that Ramanujan knew to be true. Deriving the formulas has often been more illuminating than the formulas themselves. Whole new subdisciplines within mathematics have blossomed around ideas that Ramanujan put forward in a peculiar, stark isolation.

With the special excuse of his centennial year, mathematicians are gathering to discuss the implications of Ramanujan’s work at meetings in the United States and India. They have far more raw material to work with than ever before, because the last decade has brought a new effort to find and organize the pages that make up his legacy.

A University of Illinois mathematician, Bruce Berndt, has spent years editing the notebooks, tracking down sources and relationships and, above all, proving as many of the unproved theorems as possible. A mathematician at Pennsylvania State University, George Andrews, has been performing the same task with the so-called Lost Notebook, 130 pages of scrap paper from the last year of Ramanujan’s life.

“The work of that one year, while he was dying, was the equivalent of a lifetime of work for a very great mathematician,” said Richard Askey of the University of Wisconsin, who has collaborated with Dr. Andrews in trying to understand some of Ramanujan’s work.

“What he accomplished was unbelievable,” Dr. Askey said. “If it were in a novel, nobody would believe it.”

Ramanujan might have died in complete obscurity if he had not written a series of desperate, bold letters to English mathematicians in 1912 and 1913. By then he was 25 years old, working as a \$30-a-year clerk after several years of unemployment, unwilling to put aside his slate and formulas.

His family was Hindu, high-caste but poor. His father and grandfather before him worked as clerks for cloth merchants. Ramanujan was lucky enough to have a fairly good high school education in Kumbakonam, and he began his creative exploration of mathematics after discovering the few outdated and second-rank textbooks in the library there.

"An Unknown Hindu Clerk"

His intellect stood out clearly, but in college at Madras, about 150 miles north of his birthplace, he failed again and again to pass examinations in other subjects. In mathematics itself, he had no teacher. He worked, as the English mathematician Godfrey Harold Hardy later said, "in practically complete ignorance of modern European mathematics."

Hardy was not the first mathematician to receive a letter from this "unknown Hindu clerk," as he recalled—"at the best, a half-educated Indian." But he was the first to understand what the letter contained.

Ramanujan's letters said, in effect, I know the following . . . and I also know this . . . and, by the way, I have discovered this. He offered a carefully chosen selection of his theorems. Most were in the form of identities—statements that some familiar quantity, like π , was equal to some unfamiliar quantity, or that two unfamiliar quantities were equal.

Hardy examined them with bewilderment. A few struck chords of recognition, he said later; he thought he had proved similar statements himself. Some he thought he could prove if he tried—and he succeeded, although with surprising difficulty.

Other theorems were already known. Still others, however, "defeated me completely," Hardy said in an essay years later.

Journey to Cambridge

"I had never seen anything in the least like them before," he said. "A single look at them is enough to show that they could only be written down by a mathematician

of the highest class. They must be true because, if they were not true, no one would have had the imagination to invent them."

Furthermore, Hardy could tell that Ramanujan was holding some things back, offering specific examples of theorems for which he surely must have discovered more general versions. He arranged an invitation to Cambridge University, and in 1913 Ramanujan arrived, leaving his wife behind. He stayed for nearly six years.

The two men collaborated often. Hardy remembered a slight man, of medium height, with eyes through which some light seemed to shine. Ramanujan remained a strict vegetarian, cooking all his own food in his rooms, and when he fell mysteriously ill in 1917, Hardy thought his vegetarianism contributed to his failing health.

Shared Fascination

Years later, Hardy took some pains to dispel the idea, perhaps a by-product of subtle English racism, that Ramanujan was some sort of Asian curiosity—either an "inspired idiot" or "some mysterious manifestation of the immemorial wisdom of the East." On the contrary, in Hardy's eyes he was a deliberate rationalist, often shrewd, and not nearly so religious as his dietary habits made him appear.

They shared a fascination with numbers as almost living things, or characters in a story. They thought about round numbers, defined as numbers with only small factors, like 300, $2^2 \times 3 \times 5^2$. They worked on the question of how common such numbers are, in strict mathematical terms, and on many problems more difficult to put into words.

"A Very Interesting Number"

One day after Ramanujan fell ill, Hardy visited him in a taxicab and remarked that the cab's number had been rather uninteresting—1729, or $7 \times 13 \times 19$. "No, it is a very interesting number," Ramanujan responded, as Hardy later told the story. "It is the smallest number expressible as a sum of two cubes in two different ways." (It is the sum of $1 \times 1 \times 1$ and $12 \times 12 \times 12$, and it is also the sum of $9 \times 9 \times 9$ and $10 \times 10 \times 10$.) Hardy understood and appreciated Ramanujan more than any of his contemporaries. But even he could not see beyond the blinkers of his time and place. To him, Ramanujan's story was ultimately a tragedy—of inadequate education and of genius unguided. When he finally came to assess the

younger mathematician's work and its likely influence on the future of his subject, he expressed disappointment.

"It has not the simplicity and the inevitableness of the very greatest work," Hardy wrote in 1927. "It would be greater if it were less strange."

Few mathematicians accept that assessment today, as strangeness comes into the light and Hardy recedes into Ramanujan's greater shadow.

"Hardy thought it was a shame that Ramanujan wasn't born a hundred years earlier," Dr. Askey said. That was the great age of formulas, the era of ground-laying work by such mathematicians as Euler and Gauss. "My comment is that it's a shame Ramanujan wasn't born a hundred years later," he said. "We're trying to do problems in several variables now—the problems are harder, and it would be marvelous to have somebody with his intuition to help get started."

Not that his intuition was infallible. Ramanujan made some errors, once claiming to have found a formula for the approximate number of primes less than any given number. No such formula exists. He was too optimistic, and it was the optimism of an earlier time; by the 19th century, mathematicians had learned that some problems could never be solved, but Ramanujan's isolation shielded him from their doubts as much as from their knowledge.

In 1919, increasingly ill, having entered and left a nursing home and several sanitariums, Ramanujan returned to India. He continued to work feverishly, fighting the pain of his mysterious ailment, writing on whatever paper he could find. The next April, at the age of 32, he died.

Papers Discovered in 1976

The work of his last year, 130 unlabeled pages, came to rest at the library of Trinity College, Cambridge, where they lay in a box, along with assorted bills and letters, until Dr. Andrews of Pennsylvania State University found them in 1976. This was the Lost Notebook.

"It's a bizarre term to use for something that was in the major library of the major college in England," Dr. Borwein said, "but in terms of people appreciating its contents, it was certainly true."

Dr. Andrews found that Ramanujan had cleared a path that mathematicians had not succeeded in matching in the intervening half century. Many discoveries concerned a family of identities he called mock theta functions—"simple assertions in arithmetic," as Dr. Andrews put it, although "their implications are quite profound."

Seeds of "Ramanujan's Garden"

Such mathematics has helped drive one of the major new conceptions of theoretical physics, superstring theory, as the physicist Freeman Dyson told a Ramanujan conference last month. "As pure mathematics, it is as beautiful as any of the other flowers that grew from seeds that ripened in Ramanujan's garden," he said.

Another identity was used last year to enable a computer to calculate millions of digits of pi. It converges on the exact value with far greater efficiency than any previous method. Yet, as always, Ramanujan had merely asserted his discovery; only later did Dr. Borwein and his brother, Peter B. Borwein, prove rigorously that those millions of digits really were pi.

The applications of Ramanujan's magical-seeming formulas make mathematicians think that he was mining a deep vein of theory, the full outlines of which are not yet known. But many prefer not to dwell on just how Ramanujan was able to think as he did.

Hardy looked at Ramanujan's origins and saw a crippling neglect by an inadequate educational system cut off from European society. Still, as mathematicians realize now, Ramanujan had a decent high school, a handful of books and the traditions of a culture that allowed him to aspire to a life as a scholar.

Those looking for lessons in his brief, rich life sometimes note that now, one century later, much of the planet lacks that much.

"Ramanujan is important not just as a mathematician but because of what he tells us that the human mind can do," Dr. Askey said. "Someone with his ability is so rare and so precious that we can't afford to lose them. A genius can arise anywhere in the world."

A Mysterious Formula for Pi

Mathematicians find many of Ramanujan's formulas to be both beautiful and obscure. To their surprise, the formula above provides an extremely rapid way to calculate the value of pi, an age-old preoccupation. Only last year, a computer scientist used a version of Ramanujan's formula to calculate pi to 17 million places. Only after this success were mathematicians able to prove why Ramanujan's insight was correct.

July 14, 1987

Scientist at Work: Andrew Wiles; Math Whiz Who Battled 350-Year-Old Problem

By GINA KOLATA

Dr. Andrew Wiles is a quiet, diffident man with a shy smile. Yet he summoned the courage to invest seven years working in secret on the world's most famous math problem, a formidable challenge that has baffled the best mathematicians for more than 300 years.

Last week, despite all odds, he was able to announce that he had solved it. It was a feat that, if sustained, will catapult the 40-year-old mathematics professor at Princeton University into the ranks of his subject's giants, assuring that the pinnacle of his career had been reached and making him, instantaneously, a sort of icon.

The problem, known as Fermat's Last Theorem—and familiarly as F.L.T. to its adherents—dates to 1637. The illustrious French mathematician Pierre de Fermat scribbled it in the margin of a book, adding that he had a marvelous proof that, unfortunately, would not fit in the margin. Great and not-so-great mathematicians have been trying to prove it ever since.

Dr. Wiles's proposed proof could still turn out to have a subtle flaw, some mathematicians warn. His 200-page manuscript has not yet been published. And it will take time for experts to check it fully. But unlike the many previous claims, all of which turned out to be flawed, Dr. Wiles's work has been hailed and by the leaders of the field.

Already, in Princeton, a town where people routinely drive visitors past the house where Albert Einstein lived, Dr. Wiles's celebrity has begun. Dr. Simon Kochen, chairman of Princeton's mathematics department, said he was receiving congratulations even from strangers.

Dr. Wiles has been all but impossible to find since he announced his proof at Cambridge in England last week, so the thousands of telephone calls, computer messages, and faxes from around the world have rained in on others, like Dr. Kochen and other members of Princeton's mathematics department instead.

"I don't know what it is," Dr. Kochen said. After all, he said, mathematics is practiced by a few thousand professionals and it often seems to be of little interest to the outside world. But with Dr. Wiles's proof, he added: "It's like the human

spirit still lives. It's like listening to one of the late Beethoven quartets. It's like we live now and this happened during our lifetimes."

So why Dr. Wiles? And why now? Dr. Wiles, in an interview on Sunday at his office and at his house a few blocks away, explained that finding the proof was a matter of being in the right place at the right time. And it was a matter of being obsessed with the problem.

Fermat's Last Theorem is deceptively simple to state. It says that there are no positive whole numbers that solve the equation $x^n + y^n = z^n$ when n is greater than 2. When n is 2, solutions are easy to find. For example, $3^2 + 4^2 = 5^2$. But that, by Fermat's Last Theorem, is the end of the line. There are no solutions for when n is 3 or any greater number.

Dr. Wiles says he has been fascinated by Fermat's Last Theorem since childhood. It was the theorem that drew him into mathematics.

A Boyhood Dream

The son of a theologian at Oxford University in England, Andrew Wiles first came across Fermat's Last Theorem when he was 10 years old and saw it in a book his town's public library. He has forgotten the book's title and author, but he vividly remembers its effect. It made him want to be a mathematician and it made him want to solve the problem.

"I spent much of my teenage years trying to prove it," Dr. Wiles recalled. "It was always in the back of my mind." But once he became a professional mathematician, he said, he realized that there was a lot more to it than simply working on the problem with a teenager's enthusiasm.

The problem had foiled mathematicians from Fermat's day onward. Fermat himself proved that it was true when the n 's, called the exponents in the equations, were 4. A hundred years later, in 1780, the mathematical genius Leonhard Euler proved the theorem was true for the exponent 3, and over the next 50 years others proved it true for the cases of 5, 7 and 13. But Fermat's majestic theorem refers to an infinity of numbers. The one by one approach would never prove it.

The turning point came about a decade ago when Dr. Gerhard Frey of the University of the Saarlands in Germany suggested that Fermat's Last Theorem would follow automatically if another, seemingly unrelated, proposition were true. That proposition, known as the Taniyama conjecture, dealt with mathematical objects known as elliptical curves, a class of cubic equations that had

been intensively studied by Fermat himself, although not in connection with his theorem.

Then, seven years ago, Dr. Kenneth Ribet, a mathematician at the University of California at Berkeley, formalized Dr. Frey's suggestion, showing that if a crucial part of the Taniyama conjecture could be proved, Fermat's Last Theorem would be true.

Dr. Ribet said that the Taniyama conjecture was part of a sort of grand unified theory of mathematics. "The Taniyama conjecture is part of the vast Langlands philosophy," Dr. Ribet said. He explained that Dr. Robert Langlands, a professor at the Institute for Advanced Study in Princeton, suggested years ago that two apparently disparate fields of mathematics were actually one and the same.

The fields are algebra, which deals with equations, and analysis, which, like calculus, deals with how mathematical structures vary around the neighborhood of a point on a surface. The Langlands philosophy, Dr. Ribet said, "is a deep, far-reaching vision in mathematics." The Taniyama conjecture, he added, "is a special case of what Langlands suspected."

Dr. Ribet's proof linking the conjecture to Fermat's Last Theorem fired Dr. Wiles's imagination. It said, essentially, that you could associate an elliptic curve with a solution to the Fermat equations. If you could just show that the elliptic curve could not exist, then you could show that neither could solutions to the Fermat equations.

"I knew when I heard about Frey and Ribet's result that the landscape had changed," Dr. Wiles said. "There is no question that what they did completely changed the problem for me psychologically. Hitherto, Fermat's Last Theorem was like other problems in number theory. It would go on for thousands of years and never be solved and mathematics would hardly notice."

But, Dr. Wiles added: "What Frey and Ribet did was make Fermat's Last Theorem a consequence of a problem that mathematics could not ignore. Too much depended on it. A whole architecture of future problems depended on it. For me, that meant that the problem was going to be solved. And once I had that confidence, I couldn't let go."

The very day that Dr. Wiles heard about Dr. Ribet's result, he dedicated his life to using it to prove Fermat's Last Theorem.

He worked at home on his secret project, sitting in a barren attic office on the third floor of his Tudor-style house. No computer was necessary, and no telephone was present to intrude on the absolute silence.

"If he said he was working on Fermat's Last Theorem, people would look askance," Dr. Kochen said. "And if you start telling people who are experts, you end up collaborating with them. He wanted to do it on his own." Only one person in the Princeton mathematics department knew what was going on. That was Dr. Nicholas Katz, who agreed to serve as sort of a sounding board for Dr. Wiles. But Dr. Katz was sworn to secrecy.

"I made progress in the first few years," Dr. Wiles said. "I developed a coherent strategy." Then, he said, two years ago, he had a pivotal idea that reduced the problem to a calculation. The calculation was "one that was similar to one others had tried and hadn't achieved, but it was a problem that was doable," he said.

Dr. Wiles worked feverishly on it. "Basically, I restricted myself to my work and my family," Dr. Wiles said. "I don't think I ever stopped working on it. It was on my mind all the time. Once you're really desperate to find the answer to something, you can't let go," he said.

Eventually, Dr. Wiles said, he had solved all but one critical case for his proof. The final barrier fell about six weeks ago when Dr. Wiles was reading a paper by Dr. Barry Mazur, a mathematician at Harvard University. "I can't even remember why I was looking at it," Dr. Wiles said. But he took notice of the mention of a certain construction. "It was immediately clear to me that I should use this construction and that I would solve this last problem I had."

The construction, as it happened, was not new. It dates to the 19th century. But Dr. Wiles had not heard of it before. As soon as he saw it, Dr. Wiles said, "I knew I had it." He could complete his seven-year quest and the proof of Fermat's Last Theorem.

Dr. Wiles presented his work in three lectures that he gave last week at a small mathematics meeting at Cambridge University in England.

Unlike many scientists who trumpet every tiny advance in papers and press release, Dr. Wiles gave no hint of the bombshell he was about to detonate over the world of mathematics. The audience was not even certain he would mention Fermat, though some had their suspicions from the drift of the argument. Between lectures, e-mail messages started flashing between England and the United States as mathematicians speculated on his target.

One reported, "Andrew gave his first talk today. He did not announce a proof of Taniyama-Weil but he is moving in that direction and he still has two more lectures. He is still being very secretive about the final result."

Dr. Kochen, waiting back in Princeton, was tense with anticipation. He and another Princeton mathematician, Dr. John Conway, could talk of nothing but whether the proof would be accepted by the handful of mathematicians who understood the field.

"Tuesday night, neither of us could sleep," Dr. Kochen said. Around 5:30 Wednesday morning, Dr. Conway unlocked the door to Fine Hall, the brown tower that houses the mathematics department, went into his office, and turned on his computer. The first message arrived at 5:53 a.m. from Dr. John McKay of Concordia University in Montreal, who was attending the meeting. "F.L.T. proved by Wiles," it said.

Not until the end of the third and last lecture had Dr. Wiles cited the proof in which his argument culminated.

Dr. Wiles arrived home on Friday. On Sunday, elated but tired, he said that he had spent his time with his wife and young daughters. "I've been to the swings," he said, and to a party given by friends. He has tried to absorb the consequences of his achievement.

It is also a release to have completed the proof. "I haven't let go of this problem for nearly seven years. It's gone on on a day-to-day basis. I've almost forgotten the experience of getting up and thinking about something else," he said.

Yet the release is accompanied by a bittersweet feeling at seeing this most famous of all mathematics problems vanish.

There is a certain sadness in solving the Last Theorem, Dr. Wiles said. "All number theorists, deep down, feel that," he said. "For many of us, his problem drew us in and we always considered it something you dream about but never actually do." Now, he said, "There is a sense of loss, actually."

June 29, 1993

Scientist at Work: Leonard Adleman; Hitting the High Spots of Computer Theory

By GINA KOLATA

There is nothing to look at in Dr. Leonard Adleman's office at the University of Southern California, no clue that the office is even occupied. There are no pictures of his wife or of his three daughters, no cartoons or mementos—just a computer, two chairs, a desk and a blackboard. And that is fine with Dr. Adleman. For although he is an active faculty member at the university, although he is a devoted husband and father, his is a life of the mind.

It is a life that is nourished by deep philosophical questions and the overarching beauty of mathematics. It is a life that involves days, weeks, months of pure thought, alone in his equally barren office at his home in Northridge, Calif., 30 miles from the campus. And it is a life that has led Dr. Adleman to play a central role in some of the most surprising, and provocative, discoveries in theoretical computer science.

Dr. Adleman is perhaps best known for a project that he only reluctantly got involved in. He says now that he failed to understand its significance at the time. The discovery, which he made with two other researchers, was of an entirely new sort of encryption system that changed investigators' thinking about what it meant for a code to be unbreakable.

After that, Dr. Adleman invented a new way of demonstrating that a number was prime, based on a probabilistic mathematical proof that challenged the notion, dating to the ancient Greeks, that a proof must offer utter certainty.

It was one of Dr. Adleman's students who invented the first computer virus, and Dr. Adleman who coined the term "computer virus."

And, in one of the few disappointments of his career, he hit upon an idea for slowing the loss of the white blood cells in people with AIDS, based on an analysis of graphs of the decline of immune system cells in those infected by the human immunodeficiency virus. Although Dr. Adleman is still sure he was right, he failed to communicate his enthusiasm to the medical community.

Last month, in a pioneering experiment that astonished computer scientists, Dr. Adleman combined his knowledge of two fields and published a paper

showing that DNA, the biological material, could be used as a computer, solving a math problem with a laboratory experiment.

Dr. David Jefferson, a computer scientist at the University of California at Los Angeles, said he was "incredibly impressed" by Dr. Adleman's accomplishments, especially because Dr. Adleman works alone most of the time. "It is rare to make contributions in several fields and work alone," Dr. Jefferson said.

Yet despite his successes in a field on the borderline between mathematics and computer science that seems made for him, Dr. Adleman, 48, floundered for years trying to decide what he wanted to do with his life. When he finally fell into mathematics and theoretical computer science it happened almost by chance.

Dr. Adleman grew up in San Francisco. His father was an appliance salesman and his mother a bank teller. He did not have any great ambitions for himself and, in fact, never even thought about becoming a mathematician. It was not until he took a high school course in Shakespeare that he even realized the beauty of ideas. "I was an incredibly naive and immature kid," he said, but when he took that class, and, in particular, when he read Hamlet, the teacher, "opened my eyes to the fact that one could see things more deeply than the purely superficial." He enrolled at the University of California at Berkeley only because his Shakespeare teacher suggested it.

At Berkeley, he at first declared he was going to be a chemist, inspired by years of watching Mr. Wizard on television, and then changed his mind and said he would be a doctor, inspired by his Kappa Nu fraternity brothers who wanted to be doctors. Finally, he settled on a mathematics major. "I had gone through a zillion things and finally the only thing that was left where I could get out in a reasonable time was mathematics," he said.

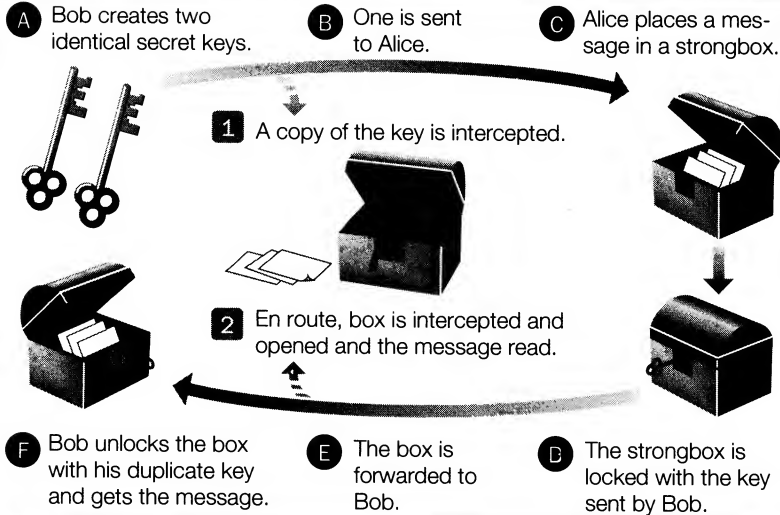
Dr. Adleman graduated in five years, in 1968, "wondering what I wanted to do with my life." He took a job as a computer programmer at the Bank of America, and soon after applied to medical school. He was accepted but changed his mind and did not enroll. Then, he said, "I decided maybe I should be a physicist," so he began taking classes at San Francisco State College while working at the bank.

Once again, Dr. Adleman lost interest. "I didn't like doing experiments, I liked thinking about things," he said. So he simply stopped going to class. Afraid that incompletes turning to F's would hurt him later, he took a book on computer science out of the college library and never returned it, figuring that the college would not send out a transcript if a student had an unpaid library fine. "I've felt

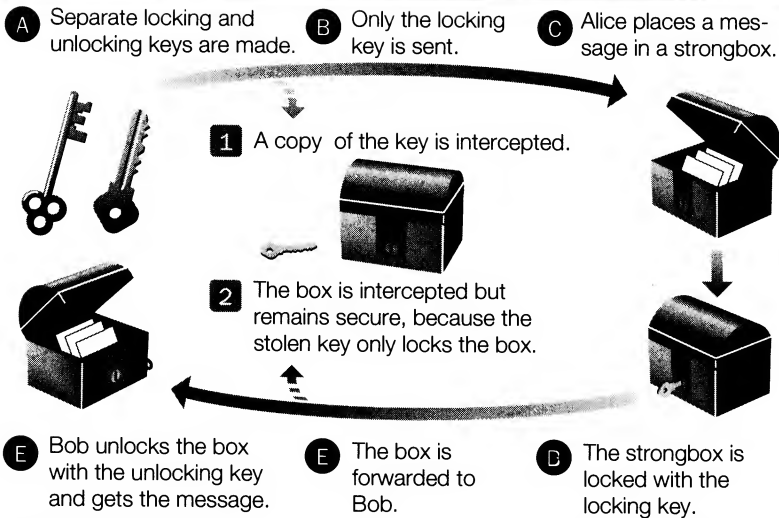
A New Way to Foil Electronic Spies

Dr. Leonard Adleman's approach to encryption used "keys" in the form of mathematical formulas that are easy to compute in one direction, but believed to be impossible for an outsider to reverse.

Traditional cryptography fails ...



... where public-key cryptography succeeds



Source: Dr. Leonard Adleman

The New York Times; illustration by Frank O'Connell

guilty ever since," he said. "Maybe I should send the college an anonymous gift."

Finally, he returned to Berkeley, with the aim of getting a Ph.D. in computer science. He had two motivations. One was practical. "I thought that getting a Ph.D. in computer science would at least further my career," he said.

The second was more romantic. Dr. Adleman had read a column in *Scientific American* by Martin Gardner on one of the most profound mathematical discoveries of the 20th century, a theorem by Kurt Gödel, and was overwhelmed by the deep philosophical implications. Gödel had shown that there are some truths that can never be verified and some untrue statements that can never be proved false. He showed that no matter how mathematicians design a logical system of axioms, there always will be some statements that are outside the system and beyond the reach of its logic.

"I thought, 'Wow. This is so neat,'" Dr. Adleman said. "There were several things I found neat—black holes, general relativity. I thought that for once in my life, I want to really understand one of these deep results." When he went to graduate school this time, he decided, he would come away understanding Gödel's result at a level beyond the superficial.

But while in graduate school, something else happened to Dr. Adleman. He finally understood the true nature and compelling beauty of mathematics. He discovered, he said, that mathematics "is less related to accounting than it is to philosophy."

"People think of mathematics as some kind of practical art," Dr. Adleman said. But, he added, "the point when you become a mathematician is where you somehow see through this and see the beauty and power of mathematics."

Dr. Adleman got his Ph.D. in 1976 and immediately landed a job as an assistant professor of mathematics at the Massachusetts Institute of Technology. (His father advised him to stay with Bank of America, where at least they had a good retirement plan.)

One day, soon after he arrived, he walked into the next-door office of Dr. Ronald Rivest. Dr. Rivest was gripped by an article that had just appeared in an electrical engineering journal, *IEEE Transactions on Information Theory*. The paper, by Dr. Martin Hellman, a computer scientist at Stanford, and his student Whitfield Diffie, described an idea for a new sort of encryption system. All previous schemes had relied on secret "keys"—formulas for scrambling messages and unscrambling them. Anyone who had a key to encrypt could also decrypt by simply reversing the encryption instructions. But Mr. Diffie and Dr. Hellman had

a revolutionary idea. They proposed using one-way functions—mathematical formulas that are easy to compute one way but impossible to reverse unless you have some special knowledge of how they were constructed. You could make your encryption key public so anyone could send you an encoded message. But only you would have the key to decoding it.

Dr. Rivest announced that he would find such a one-way function and create a public key cryptosystem. Although it seemed clear that the idea should work, finding a one-way function that was truly one-way was not so easy. Dr. Adleman greeted the idea with a polite yawn, thinking it impractical and not very interesting. Nonetheless, Dr. Rivest and another colleague, Dr. Adi Shamir, now at the Weizman Institute of Science in Israel, were truly excited by the concept.

"They would talk endlessly about it and because we were all together so much, we would discuss it," Dr. Adleman said. Soon Dr. Rivest and Dr. Shamir were trying to invent an unbreakable public key system. Dr. Adleman's role was to test each proposed system by trying to break it. Dr. Rivest and Dr. Shamir invented 42 coding systems and each time Dr. Adleman broke the code.

Late one night, following a Passover dinner, Dr. Rivest called Dr. Adleman with the 43d idea, this one based on a difficult factoring problem. Dr. Adleman said he thought this time the code really was unbreakable because of the mathematics involved. The number would take years or even centuries of computing to factor. The makers of the code could decrypt it because they had constructed the large number and so they knew its factors.

Dr. Rivest stayed up all night working on a manuscript describing the code and the next morning he handed it to Dr. Adleman. He had listed the paper's authors, in alphabetical order, as Adleman, Rivest, Shamir.

"I told Ron, 'Take my name off the paper. It's your work,'" Dr. Adleman said. But Dr. Rivest insisted.

"I thought, 'Well, it's going to be the least important paper I've ever been on, but in a few years I will need so many lines on my vita to get tenure,'" Dr. Adleman recalled. "And, on the other hand, I did do a substantial amount of intellectual work breaking the codes 1 through 42. So the reasonable thing to do is be the third author."

Mr. Gardner wrote about the code, now called R.S.A. for the names of its authors, in his column. To Dr. Adleman's astonishment, the investigators and their code were instantly famous. Thousands of people wrote to them. "It just shocked us," Dr. Adleman said. The National Security Agency, which until then

had been essentially the only place where encryption was studied and had kept its work secret, complained that the publication of seemingly unbreakable codes like R.S.A. could endanger national security.

"People kept telling me I was going to get rich," Dr. Adleman recalled, so he went out and bought a new car, a red Toyota, a hopeful investment since he was making just \$13,000 a year at M.I.T.

The three investigators assigned the patent for their code to M.I.T. and in 1983 formed a company, R.S.A. Data Security Inc. of Redwood City, Calif., to make R.S.A. computer chips. "I was the president, Ron was chairman of the board, and Adi was treasurer," Dr. Adleman said. He still owns stock in the company, but, he said, after he "drove the company into the ground," he no longer is an officer. The R.S.A. chips are widely used, but the privately held company has yet to make anyone rich.

Although he was intellectually stimulated at M.I.T., Dr. Adleman longed for California and he wanted to marry and have a family. So, in 1980, he took a job at the University of Southern California and left for Los Angeles. Three years later, he met his future wife, Lori Bruce, at a singles dance. "It was love at first sight," Dr. Adleman said, and the two were married six weeks later.

The first computer virus was born on Nov. 11, 1983, when one of Dr. Adleman's students, Fred Cohen, told Dr. Adleman he had a new idea for a computer security threat and asked if he could use the university's computers to try it out. "The second he described it to me, I thought there was no point in doing the experiment," Dr. Adleman said. "It was obvious it would work."

Dr. Adleman named the program a computer virus and had long, agonizing discussions with Mr. Cohen about the ethics of its creation. Finally, they decided that it was best to publicize the viruses to warn people that such programs could be made. Mr. Cohen set his virus loose and it quickly spread throughout the university's computers. Mr. Cohen wrote his Ph.D. thesis on computer viruses.

Dr. Adleman's mode of working is to find something that intrigues him and to dig in. He does not read mathematics journals, he says, because he does not want to be influenced by other people's ideas.

When he decided, recently, to see if he could use DNA, the genetic material, as a computer, he spent a year in a molecular biology lab learning the techniques and what experiments were possible. He wanted to translate a mathematical problem into the language of biology and then exploit the incredible efficiency and speed of biological reactions to solve it. He spent six months thinking of the

perfect problem to ask DNA to solve before deciding upon a problem involving finding a path connecting seven cities. And once he found the problem, it was like the computer virus. The actual experiment was superfluous. It was obvious that it would work, he said. But he did the experiment anyway, to enhance his chances of getting the paper published. His paper describing the work appeared in the journal *Science* on Nov. 11.

Asked what it is like to simply sit and think for six months, Dr. Adleman responded: "That's what a mathematician always does. Mathematicians are trained and inclined to sit and think. A mathematician can sit and think intensely about a problem for 12 hours a day, six months straight, with perhaps just a pencil and paper." The only prop he himself needs, he said, is a blackboard to stare at.

December 13, 1994

Dr. Kurt Gödel, 71, Mathematician

By PETER B. FLINT

Dr. Kurt Gödel, regarded by some mathematicians as the world's leading logician, died yesterday at the Medical Center in Princeton, N.J. He was 71 years old and lived at 145 Linden Lake in Princeton.

Dr. Gödel formulated Gödel's Theorem, which became a hallmark of 20th-century mathematics and generated tremendous strides in mathematical logic and the foundations of modern mathematics.

The theorem states that in any rigidly logical mathematical system there are propositions or questions that cannot be proved or disproved on the basis of the axioms within that system and that, consequently, it is not certain that the basic axioms of mathematics will not raise contradictions.

The scholar had formulated the theorem in 1931 while he was teaching at the University of Vienna. He was also a member of the Institute for Advanced Study in Princeton in 1933 and 1935 and from 1938 to 1952. He became a professor there in 1953 and retired in 1976 as professor emeritus.

"More Than a Monument"

In 1951, Dr. Gödel was the co-recipient of the first Albert Einstein Award for achievement in the natural sciences. The award has been termed the highest of its kind in the United States. His work in mathematical logic, according to the awards committee composed of distinguished scientists, constitutes "one of the greatest contributions to the sciences in recent times."

In presenting the award, Dr. John von Neumann of the institute said, "Kurt Gödel's achievement in modern logic is singular and monumental—indeed it is more than a monument, it is a landmark which will remain visible far in space and time."

Gödel "was the first man to demonstrate that certain mathematical theorems can neither be proved nor disproved with the accepted, rigorous methods of mathematics. In other words, he demonstrated the existence of undecidable mathematical propositions. He proved, furthermore, that a very important specific proposition belonged to this class of undecidable problems—the question as

to whether mathematics is free of inner contradictions. The subject of logic will never be the same."

The logician won many honorary doctorates from major institutes. A citation from Harvard described him as the "discoverer of the most significant mathematical truth of this century, incomprehensible to laymen, revolutionary for philosophers and logicians."

January 15, 1978

Genius or Gibberish? The Strange World of the Math Crank

By GEORGE JOHNSON

The letter, dated Christmas Day 1998 and addressed to a professor at the Niels Bohr Institute in Copenhagen, began portentously: "Nowadays, we seek to comprehend our comprehensions and call that comprehensiveness knowledge in the mistaken belief that as a science it is immortal. Such omniscience diffuses like Helium-3 into the penetralia mentis of omnipotent impotency within any God-head such that any caveat actor is saved. . . ."

Within a few sentences, the writer was holding forth on Heisenberg's Uncertainty Principle and "the concept of nothing" as the empty set, before launching into speculations involving number theory: "It's enough to make me conjecture that infinity's prime and Riemann's Zeta function accounts for fractional charge subatomically just for the Higg's boson with an involucral matrix of ogdoad parity as midwife!"

The letter was typed single-spaced with the tiniest of margins and embellished with hand-drawn diagrams and colored annotations. Copies were sent to a list that included the linguist Noam Chomsky, the physicists John Archibald Wheeler, David Deutsch and Stephen Hawking, and the mathematician John Casti.

"It has all the hallmarks of a crank," said Dr. Casti, who is affiliated with the Technical University of Vienna and the Santa Fe Institute in New Mexico. "It's amazing all the stuff you can get onto a single piece of paper."

But was it not just possible that couched in the obscure mix of mathematics, physics and Egyptian mysticism ("ogdoad parity" refers to four pairs of gods with names like Darkness, Absence and Endlessness), there lay an important insight?

Didn't two Cambridge University mathematicians dismiss the great self-taught Indian number theorist Srinvasa Ramanujan as a crackpot when he sent them long eccentric letters from India early in this century? Only their colleague G. H. Hardy had the foresight to recognize Ramanujan as a genius. And didn't the great German mathematician Carl Friedrich Gauss foolishly throw away unread a groundbreaking paper from his young Norwegian colleague Niels Henrik Abel, calling it "another of those monstrosities"?

Dr. Casti was not too worried about the possibility. Though the stories of Ramanujan and Abel may linger in the backs of mathematicians' minds as they aim the latest unsolicited epistle toward the wastebasket, most become quickly jaded.

"After several hundred of these things you get into that mode," said Dr. Ian Stewart, a mathematician at Warwick University in England. "It has to do with your self-preservation.

"The writers of these letters range from pretty good amateur mathematicians who have made a mistake somewhere or skipped over an important step to people who are completely mad," he said. "You get very strange mail in 17 different fonts and 14 colors and with an idiosyncratic grammar." Many of the correspondents are intelligent, well-meaning, indefatigable souls who, in their untrained way, share the fascination mathematicians feel for the invisible world of numbers. And many are simply cranks.

The equipment necessary for discovering a subatomic particle in your own home costs too much and would never fit inside a basement laboratory or even a very large backyard. But with nothing more than a pencil and paper, and maybe a compass and straightedge, even an amateur can explore the mathematical nether world, stumbling across important new truths.

That, anyway, is the dream or obsession that drives would-be Ramanujans all over the world to send mathematicians letter after letter crammed full of diagrams and equations promising answers to unsolved problems ranging from squaring the circle or proving (in a simpler way) Fermat's Last Theorem to revealing, through the wonders of mathematics, the meaning of life.

Physicists get their share of mail from amateurs attempting to reconcile quantum mechanics and general relativity or to show that Einstein was wrong. But the greater ease with which one can speculate about numbers has caused the mathematical crank to become enshrined in academic folklore. The phenomenon is even documented in a book called *Mathematical Cranks* (Mathematical Association of America, 1992), by Dr. Underwood Dudley, a mathematician at DePauw University in Indiana.

"I've been at this for a decade and still can't pin down exactly what it is that makes a crank a crank," said Dr. Dudley, who has met a few in person. "They are usually men, old men," he said. "All are humorless. None of them are fat," a characteristic he attributes to their obsessive personalities. "It's like obscenity—you can tell a crank when you see one."

With recent films like *Good Will Hunting* and *Pi* giving mathematics a romantic sheen and popular new biographies romanticizing the lives of the mathematicians Paul Erdos and John Nash, the flow of crank mail will only increase, predicted Dr. John Allen Paulos, a mathematician at Temple University in Philadelphia.

Add millennial anxiety, including the Y2K problem, Dr. Paulos speculated, and the time he and his colleagues spend opening and discarding letters peppered with strange symbols and grand claims is bound to increase. "Popular mathematics used to be an oxymoron," he said, "but happily that's not true anymore." The celebrity, though, has its price.

"It's a real dilemma," said Dr. Reuben Hersh, professor emeritus of mathematics at the University of New Mexico in Albuquerque. "Who is going to stroll through pages and pages of stuff that is very hard to understand when you don't have to do it? From the point of view of these guys, we are arrogant, unwilling to reconsider ideas. And why shouldn't they expect a responsible scientist to look carefully at some new idea that might be important?"

"You can't just say Ramanujan was a genius and these other guys were cranks," Dr. Hersh said. "With a superficial look, there is hardly any visible difference. There is not always a sharp line between eccentric mathematicians and intelligent but maybe obsessed amateurs."

Until recently much of the mail contained supposed proofs of Fermat's Last Theorem. But since Dr. Andrew Wiles of Princeton University recently proved this famous puzzle and number theory, Dr. Paulos said, the focus has shifted to disproving Dr. Wiles. Another favorite diversion is Goldbach's Conjecture, which holds that all even numbers are the sum of two primes. Though no one has found a counter example, this would-be theorem remains unproven, unless the solution has been crumpled up in a math department wastebasket somewhere.

Mathematicians are especially impatient with letters claiming to have solved one of the three classical problems of Greek mathematics: trisecting an angle (dividing it into three equal parts), doubling a cube, or squaring a circle (constructing a square with the exact same area as a circle) using only a compass and an unmarked straightedge. The reason for imposing these restrictions was to see how much mathematics could be derived from two basic concepts, the line and the circle.

Solving the three classic problems this way has been proved impossible. In 1882, for example, the German mathematician Ferdinand Lindemann established

that trying to square the circle was hopeless. The reason is that pi, the ratio of the circumference of a circle to its diameter, is not only irrational (its infinitely long string of decimal places never repeats) but transcendental (it is not a solution of any polynomial equation with whole number coefficients).

Amateur attempts at squaring the circle generally amount to rounding off pi to a close approximation like $22/7$ or $355/113$. At best the result is a square that is very close but never exactly the size of the circle.

"These people don't know what impossible means," Dr. Dudley lamented. "They think it just means very hard."

Or the writers do not believe the impossibility proofs. "They start by saying they know there is a theorem that says it is impossible but they've done it anyway, so there must be something wrong with the theorem," Dr. Stewart said. "They are operating in a conceptual vacuum. It leads to strange things."

One of the rules mathematicians soon learn is never to answer a possible crank. The mail often comes with cover letters assuring that the work has been "endorsed" by a certain Harvard or Stanford professor, say, or even a member of the United States Senate. The attached letters are usually no more than polite brushoffs: "Thank you for your interesting letter. . . ." A mathematician who makes a perfunctory reply can count on its being stapled to the next round of mailings.

Dr. Hersh replied to a letter from an amateur mathematician in India. "This guy wrote very well," he said, "in a good expository style. His penmanship was fine. What he said made enough sense that I thought I would try to explain and straighten him out."

Over several years, Dr. Hersh realized that his correspondent had come to believe that the whole edifice of mathematics was about to crumble because of a dreadful mistake made centuries ago. Dr. Hersh finally wrote back in exasperation: "I've done all I can for you. I can't do anymore." The writer answered that he did not consider himself Dr. Hersh's student but rather his opponent in a debate.

Surprisingly, the rise of the Internet has not increased the amount of mathematical crank mail. Most of the letters still come typewritten, often on what appear to be manual typewriters. "Cranks are always about one level of technology behind," Dr. Dudley said. Dr. Casti said he imagined some of his correspondents as "penniless guys in cold-water flats." They save paper and postage by single-spacing and often type on both sides of the page.

Sometimes, just sometimes, a mathematician finds that it pays to answer an unsolicited letter, one that does not have what Dr. Stewart calls "the strange fairy

dusting of lunacy." He once received a clearly written letter from a man in China who believed he had trisected the angle. "I knew it had to be a fallacy, but it gave me a spur to try and see where it was wrong," Dr. Stewart said. "There were three points in the diagram that looked as if they were on a straight line, but actually were not." Dr. Stewart wrote back and received a reply thanking him for pointing out the error. "It is the only time I've had any success convincing someone like this that they were wrong," he said.

Several years ago Dr. Stewart heard from a man—in India again—who had found a new, simpler proof for an obscure, pointless theorem in number theory written by Ramanujan and a collaborator. According to the Ramanujan-Nagell theorem, the only numbers one can square and add 7 to, yielding an answer that is a power of 2, are 1, 3, 5, 11 and 181. For example, squaring 3 and adding 7 gives 16, which is the fourth power (the square of the square) of 2.

Dr. Stewart was surprised to realize that the proof was correct, but it was badly typed on strange paper and cast in an idiosyncratic style that would have given any journal editor the impression that the writer was a crank. Dr. Stewart advised the writer to find an Indian number theorist who could teach him how to present a proper paper. Several years later the result was published, and soon after came another publication from the same man. "It is worth reading these things occasionally," Dr. Stewart said.

But only occasionally, Dr. Dudley advised. "There is always that chance of success, but it is so small," he said. "I've gone through enough reams of crank stuff to know that the probability is close to zero."

February 9, 1999

CONTRIBUTORS' BIOGRAPHIES

Lisa Belkin is a senior columnist on Life/Work/Family at the *Huffington Post*. She was previously at *The New York Times*, where she was a national correspondent based in Houston, a medical reporter, a contributing writer for *The New York Times Magazine*, and the creator of the Life's Work column and the Motherlode blog.

Malcolm W. Browne (1931–2012) was a longtime science writer for *The New York Times* who won a Pulitzer Prize in 1964 for his coverage of the Vietnam War for the Associated Press. His 1963 photograph of the self-immolation of a Buddhist Monk became one of the most memorable images of the conflict.

Kenneth Chang is a science reporter for *The New York Times*.

Ingfei Chen is a freelance health reporter whose work has been published in *The New York Times*, *Discover*, *Reader's Digest*, and others.

Anne Eisenberg is a longtime technology reporter who currently writes the Novelties column for *The New York Times*.

Peter B. Flint (1928–1995) was a reporter for *The New York Times* who specialized in obituaries of film and theater figures and other notables.

James Gleick is an author, journalist, and biographer whose best-selling books include *The Information: A History, a Theory, a Flood* (2011) and *Chaos: Making a New Science* (1987). Three of his books have been Pulitzer Prize and National Book Award finalists.

Jascha Hoffman has written on science and culture for *The New York Times*, *Nature*, and other publications. He lives in San Francisco and is also a songwriter.

Paul Hoffman is the host of the PBS television series *Great Minds of Science*, and the president and CEO of Liberty Science Center in Jersey City, New

Jersey. He is also the author of several books including *King's Gambit: A Son, a Father, and the World's Most Dangerous Game* (2007) and the international bestseller *The Man Who Loved Only Numbers: The Story of Paul Erdős and the Search for Mathematical Truth* (1999). He was formerly the editor in chief of *Discover*, the president and publisher of *Encyclopedia Britannica*, and is a puzzle master (under the pseudonym Dr. Crypton) and a class-A level chess player.

George Johnson is a science writer and the author of a number of books, including *The Ten Most Beautiful Experiments* (2008) and *Strange Beauty: Murray Gell-Mann and the Revolution in 20th-Century Physics* (1999).

David Cay Johnston is an investigative journalist and author specializing in economics and tax issues. He won the 2001 Pulitzer Prize for Beat Reporting while at *The New York Times*. He is the author of several best-selling books including *Free Lunch: How the Wealthiest Americans Enrich Themselves at Government Expense (and Stick You with the Bill)*, and since 2009 he has been a Distinguished Visiting Lecturer at Syracuse University College of Law and Whitman School of Management.

Gina Kolata reports on science and medicine for *The New York Times*. She is also a frequent lecturer, a two-time Pulitzer Prize finalist, and the author of several books include *Rethinking Thin: The New Science of Weight Loss and the Myths and Realities of Dieting* (2007), which was a finalist for the Quill book awards; and *Flu: The Story of the Great Influenza Pandemic of 1918 and the Search for the Virus that Caused It* (1999).

William L. Laurence (1888–1977) was a science writer for *The New York Times*. He received two Pulitzer Prizes, and, as the official historian of the Manhattan Project, was the only journalist to witness the 1945 Trinity test of the atom bomb in New Mexico and, shortly after, the nuclear bombing of Japan.

Henry L. Lieberman (1916–1995) was a foreign correspondent and later an editor in charge of science news for *The New York Times*.

Will Lissner (1909–2000) was a reporter for *The New York Times* from 1926 until he retired in 1976.

Steve Lohr is a technology reporter for *The New York Times* and is co-author of *U.S. vs. Microsoft* (2000). He was nominated for a Pulitzer Prize in 1998 for his coverage of Microsoft and its antitrust battle with the United States government.

John Markoff is a science correspondent for *The New York Times* and the author of *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry* (2006).

Pradeep Mutalik is a scientist at the Center for Medical Informatics at Yale University. He trained as a physician and has written on neurophysiology, animal behavior, computer science, artificial intelligence, radiology, mysticism, and consciousness.

John A. Osmundsen, a former science reporter for *The New York Times*, is the author of a number of books, including *Sweet Reason: On Life, Love and War in the Nuclear Age*.

Dennis Overbye is a science reporter for *The New York Times* and author of *Lonely Hearts of the Cosmos: The Scientific Search for the Secret of the Universe* (1991) and *Einstein in Love* (2000).

John Allen Paulos is a professor of mathematics at Temple University, and the author of *Innumeracy: Mathematical Illiteracy and its Consequences* (1988) and *A Mathematician Reads the Newspaper* (1995).

Sara Robinson is a journalist who has covered mathematics, computer science, economics, and technology for a number of newspapers and magazines, including *The New York Times*.

Bruce Schechter is a physicist, science writer, and author of *My Brain Is Open: The Mathematical Journeys of Paul Erdős* (1998).

Richard Severo was a *New York Times* reporter from 1968 until retiring in 2006.

Sidney Shalett (1911–1965) was a journalist who wrote for the *Chattanooga Times* and *The New York Times*, and was a Washington correspondent for *American Magazine*.

Leonard Silk (1918–1995), who had a Ph.D. in economics, was a columnist and editorial writer for *The New York Times* and *Business Week*.

Janet Stites is a journalist and consultant specializing in science, technology, and business. She was the founder and publisher of tech/finance magazine *AlleyCat News*. She and has written for *Portfolio Magazine*, *AllBusiness.com*, *Fortune Small Business*, and the *Bulletin of the Santa Fe Institute*.

Walter Sullivan (1918–1996) was an award-winning science reporter and editor for *The New York Times* and during his fifty-year career was considered the dean of science writers.

Clive Thompson is a Canadian journalist who writes about the social and cultural impact of digital technologies for a number of publications, including *The New York Times Magazine* and *Wired*.

John Tierney writes the Findings column for the *Science Times* section of *The New York Times*. He is the co-author, with Roy Baumeister, of *Willpower: Rediscovering the Greatest Human Strength* (2011).

Bina Venkataraman designs and leads international projects and helps shape the nation's science and technology policy agenda. She teaches at MIT and writes for publications including *The New York Times* and *The Boston Globe*.

Peter Wayner, who contributes frequently to *The New York Times*, is the author of several books on technology, including *Disappearing Cryptography: Information Hiding*.

Joseph Williams is a former editor in the business section of *The New York Times*.

PHOTOGRAPHY and ILLUSTRATION CREDITS

Page 40, heavy object rising to top, illustrations by *The New York Times*.

Page 51, census taker, photo by Cheryl Gerber.

Page 54, elderly man, illustration by Stuart Goldenberg.

Page 92, charts, illustrations by Jessica Hagy.

Page 119, rabbit, illustration by Xianfeng David Gu and Shing-Tung Yau.

Page 165-166, fingers, number sets, and subsets, illustrations
by *The New York Times*.

Page 175, knots, illustration by Joan S. Birman.

Page 188, bubbles, photo by Tony Cenicola.

Page 345, Nick Patterson, photo by Jonathan Player.

Page 349, Ali Shamir, photo by Gabriel Bouys/AFP/Getty Images.

Pages 364-366, 368, 370-373, 375, and 377, illustrations
by Charles E. McDonnell.

Page 424, Terence Tao, photo by Monica Almeida Monica.

Page 452, treasure chest, Frank O'Connell.

ACKNOWLEDGMENTS

The editor would like to thank Baden Copeland, Mika Grondahl and Frank O'Connell for their help with graphics; Peter Morance for his work on the illustrations; and Phyllis Collazo for her photography research.

INDEX

A

Aaronson, Scott, 417
 Abel, Niels Henrik, 458–459
 Adams, Jeffrey, 190, 191
 Adams, John, 99, 100, 289
 Adleman, Leonard, xv, 449–455
 background and education, 450–452
 computer virus origin and, 449, 454
 DNA as computer, 450, 454–455
 encryption “keys” approach, illustrated, 451. *See also* R.S.A. system and
 on Fermat’s Last Theorem solution, 145
 idea for slowing AIDS, 449
 N.S.A. financing and, 307
 R.S.A. system and, 27, 308–309, 310, 452–455
 secret code of, xv, 27
 Aggregation problems, 66, 70–72
 Aiken, Howard H., 361
 Aldous, David, 73, 75
 Alibek, Ken, 296
 Allen, Art, 186
 Alon, Noga, 26
 Alt, Franz L., 358
 Analytical Engine, 360, 361
 Anderson, Michael T., 122, 123, 124
 Anderson, Philip W., 262, 264
 Andrews, George, 439, 442
 Appel, Kenneth, 25, 136
 Ardan, Bach, 286, 287
 Arecchi, F. Tito, 240, 241
 Arnett, Frank, 56
 Arora, Sanjeev, 381, 383
 ARPAnet, 417
 Arrow, Kenneth J., 249, 252–253
 Arrow’s Theorem, 72
 Arthritis pain, weather and, 54–57, 291
 Arthur, James, 162–163
 Askey, Richard, 439, 442, 443
 Asteroids and moons, chaos and, 239–242

Atiyah, Michael, 10
 Atkins, Derek, 28
 Axiom of choice, 167–168

B

Babai, László, 382, 383, 384, 421
 Babbage, Charles, 360–361
 Bak, Per, 68, 69
 Ball, Sir John M., 428
 Bayer, Dave, 73, 75, 76
 Beautiful mathematics, computers and, 24–26
 Belkin, Lisa
 article by, 281–297
 biography, 463
 Benton, Michael, 68–69
 Berndt, Bruce, 439
 Berson, Thomas A., 331, 333
 Bertrand Russell and the *Origins of the Set-Theoretic “Paradoxes”* (Garcia Diego), 128–129
 Bhanot, Gyan, 392, 393
 Biham, Eli, 328, 329, 332
 Birds, flocking of, 256–260
 Birkhoff, George D., 135, 203
 Birman, Joan S., 177, 178
 Birthdays
 draft lottery, randomness and, 266
 near birthdays and, coincidences/probabilities and, 38–39, 285–286, 291–292
 puzzle problem solution, 95–101
 Blum, Lenore, 268
 Blum, Manuel, 268, 315, 382, 383
 Boardman, Norman, 303, 305
 Bobo, E. Ray, 44
 Bolds, George, 288
 Book overview, xiii–xvi
 Boole, George, 361, 371
 Borwein, Jonathan, 438, 439, 442, 443
 Boslough, Mark, 391–392
 Boyer, Robert, 20
 Braess, Dietrich, 48–49

Brains

 damaged, mathematics skills and, 5
 filling in gaps, 289
 imposing structure, 289
 mathematics concepts and, 4–8, 153–154
 patterns and, 260
 randomness, probability and, 92
 tests with rats/chimps, 5–6
 universal harmony and, 153
 unsolvable problems, 153–154
 Web as metaphor for, 107–109
 Brains, electronic. *See also* Computers
 algorithm recognizing patterns, 403–405
 Census Bureau and, 357
 development of, 356–357
 ENIAC, 357, 358–359, 361, 396, 398–399
 gathering “human intelligence,” 107–108
 math as useful invention or absolute truth or, 3–8
 war developments and, 356–357, 358–359
 Webmind, 107–109
 Brock, William A., 248
 Brooks, Jack, 335
 Browne, Malcom W.
 articles by, 67–69, 204–207, 270–273, 274–277, 303–305, 319–323, 406–409
 biography, 463
 Bryant, Robert L., 191
 Bubbles
 Plateau’s problem and, 173–174
 shape-shifting, 188–189
 surface tension, 173–174, 236
 Buck, Gregory R., 275
 Bueno de Mesquita, Bruce, 77–87
 background and education, 79, 81–82

INDEX

- Bueno de Mesquita, Bruce,
 (continued)
 C.I.A. predictions by, 84
 client secrecy and
 acquisition, 84–85
 model gone awry, 86
 people observation skills, 84
 predicting corporate events,
 82–83
 predicting how leaders
 behave, 79–80
 predicting nuclear
 capabilities of Iran,
 77–79, 87
 range of client cases, 83–84
 success of model, 85–87
 William Riker and, 79
 Burris, Stanley, 20, 22
 Bush administration, 86, 334,
 337
 Bush, Vannevar, 355
 Business, predicting corporate
 events, 82–83
 Butterfly effect, xiv, 211, 216
 Byrne, John, 336
- C**
- Campbell, David K., 184, 185,
 240, 261
 Camp, William J., 390, 391
 Candès, Emmanuel, 424
 Cantor, Georg, set theory and,
 164–168
 Cardano, Gerolamo, and
 Cardano's Method,
 92–93
 Cards, shuffling. *See* Shuffling
 cards
 Carlson, James, 124, 133
 Carnap, Rudolf, 115, 117–118
 Cartan, Élie Joseph, 115,
 116–117
*The Cassandra Prophecy:
 Armageddon
 Approaches* (Gurney),
 293
 Casti, John, 458, 459, 461
 Catastrophe theory
 about: overview of, 69,
 200–201
 chaos vs., 200
 criticism of, 204–205,
 206–207
 origins, 69
 prison system interest,
 205–206
 topology and, 69, 205
 Census-related problems,
 51–52, 53, 357
 Chaikin, Paul M., 182
 Chaitin, Gregory J., 4
 Chalmers, Leslie, 328
 Changeux, Jean-Pierre, 8
 Chang, Kenneth
 articles by, 181–183,
 188–189, 190–191,
 423–427, 428–429
 biography, 463
 Chaos and chaos theory,
 208–222. *See also*
 Stock market, chaos
 ruling
 about: overview of,
 200–201, 208
 changing course of physics,
 210–211
 child in swing example, 217
 defined, 202–203, 208, 247
 development of, 210–213
 dripping faucet and,
 209–210, 219, 220
 essence and ramifications
 of, 219–222
 examples, 209–210,
 212–213, 217
 extreme events and, 247
 fish population example,
 212–213
 fractals and. *See* Fractals
 global instability and,
 248–250
 health applications, 219–220
 moons, asteroids and,
 239–242
 patterns and, 210, 213,
 215–216, 217, 218–219,
 220
 period doubling and,
 212–213, 215–216, 220
 planets' motions and,
 202–203
 randomness and, 211,
 213, 218, 221. *See also*
 Randomness
 real-world application, 209
 "space" and, 203
 springboard for, 210
 strange attractors and,
 218–219
 turning point, 219
 vision of applications,
 219–222
Chaos (Gleick), 200
 Chartrand, Gary, 26
 Chen, Elizabeth, 182, 183
 Chen, Ingfei
 article by, 345–348
 biography, 463
 Chislenko, Alexander, 109
 Cholesterol-lowering drugs,
 32, 410
 Chomsky, Noam, 458
 Chorus-line hypothesis, 258
 Chung, Fan R. K., 14–15, 24–26
 Clinton administration, 86, 338,
 339, 341
 Clipper/Tessera technology,
 339–342
 Clusters, disease, 36, 278–280,
 292
 COBOL (Common Business
 Oriented Language),
 376, 395, 399
*Cognitive Surplus: Creativity
 and Generosity in a
 Connected Age* (Shirky),
 416
 Cohen, Fred, 454
 Cohen, I. Bernard, 223
 Cohen, Joel E., 48, 49–50
 Cohen, Marvin, 263
 Cohen, Paul J., 164, 167, 168
 Cohen, Richard J., 219–220
 Cohn, Henry, 181, 183
 Coifman, Ronald, 385, 387, 389
 Coincidences, 281–297. *See*
 also Coincidences,
 conspiracies vs.;
 Randomness
 anthologies of, 36–37
 big world, small world and,
 285, 290
 birthdays, near birthdays
 and, 38–39, 285–286,
 291–292
 "debugging human
 intuition," 290
 defined, 282
 disease clusters and, 36,
 278–280, 292
 explaining, 35–39
 finding connections and, 289
 Finnish twins' deaths,
 283–284
 Lincoln/Kennedy deaths,
 294–295
 miraculous intervention
 vs., 283

INDEX

- odds of, 283, 284
- perceived as fate, 289–290
- perception spectrum, 289
- personal attachment and, 291–292
- probability vs., 285
- weather/arthritis pain
 - relationship, 54–57, 291
- winning two lotteries, 37–38
- Coincidences, conspiracies vs.
 - about: overview of, 282–283
 - bioterror/germ warfare deaths (Que, Wiley, Pasechnik, et. al.), 281, 283, 286–288, 292–294, 295–297
 - Finnish twins' deaths and, 284
 - paranoia and, 282
 - patterns and, 282–283, 288–289
 - real conspiracies, 292
 - Sept. 11, 2001 incidents and, 282–283, 288, 292
 - Web impacting perceptions, 295
- Coin-tossing, 92, 99, 265, 270–273
- Collins, Keith, 412
- Compressing data, 385–389, 400–402
- Compton, Pat, 111
- Computers. *See also* Brains, electronic
 - about: overview of, 353–354
 - "bug" origin, 396
 - coin-tossing, 270–273
 - compressing data, 385–389, 400–402
 - conjectures and, 13–15
 - DNA as computer, 450, 454–455
 - emulating brain functions, 403–405
 - figuring out market, 107–109
 - fluid math simplified by, 243–245
 - Frances E. "Betty" Holberton and, 398–399
 - health care debate, mining patient records, 410–414
 - impact and uses, 362–363
 - linear programming problems, 407–408
 - mathematicians embracing, 16–18
 - P-NP challenge, 351–352, 415–417
 - predicting nuclear capabilities of Iran, 77–87
 - Rear Adm. Grace Hopper and, 395–397
 - security issues. *See* Cryptography
 - seeking truths, 13–15
 - shortcut for checking long proofs, 381–384
 - showing reasoning power, 19–23
 - solving difficult problems more efficiently, 406–409
 - storing images more efficiently, 385–389
 - supercomputers, 190, 243, 244, 321, 390–394
 - traveling salesman problem and, 351, 352, 353, 407
 - virus invention, 449, 454
- Computers, origins and mechanics of, 360–380
 - Analytical Engine, 360, 361
 - binary system, 365–366, 370
 - block diagram, 374–375
 - Charles Babbage and, 360–361
 - clock function, 373–374
 - coded information systems, 363–375
 - Difference Engine, 360
 - early years, 355–362
 - ENIAC (1940s), 357, 358–359, 361, 396, 398–399
 - "flip-flops" defined, 369
 - gates, 372–374, 375
 - input devices, 367. *See also* punch cards and
 - inventory control processing example, 364–365, 367, 372–373, 376–379
 - key players in, 361
 - logical operations, 371–373
 - memory addresses, 376–379
 - memory (storage) systems, 367–369
 - pulse-producing "machine," 366
 - punch cards and, 359, 360, 362
 - registers, 369
 - software development, 364–365
 - source languages, 375–380
 - stored-program concept, 361–362
 - "thinking machine" or "product integrator" (1927), 355
- Condon, Edward U., 356, 357
- Condon, Suzanne, 279
- Conjectures, computers and, 13–15
- Connes, Alain, 8
- Conn, Michael S., 337
- Conrey, Brian, 190, 191, 192
- Conversations on Mind, Matter and Mathematics*, 8
- Conway, John H., 181, 182, 419, 430–435, 448
- Cosgrave, Paul J., 110–111, 112
- Counting and aggregating, 70–72
- Cozzarelli, Nicholas R., 179
- Cranks, strange world of, 458–462
- Cray supercomputers, 243, 244, 321
- Cryptography, 343–344. *See also* National Security Agency (N.S.A.)
 - about: overview of, 301–302
 - Adleman "keys," illustrated, 451. *See also* R.S.A. system
 - breaking encryption standards, 328–330, 331–333, 343–344
 - Clipper/Tessera technology, 339–342
 - code keys control controversy, 334–337
 - Cryptos package, 336
 - Data Encryption Standard (D.E.S.), 328–330, 331–333
 - factoring 100-digit number and, 319–323
 - factoring 155-digit number and, 324–327

INDEX

- Cryptography, (*continued*)
 512-bit system, 343–344
 guarding secret keys, 320
 harassment alleged over
 research, 303–305
 math and, 316–317
 PC chip security, 349–350
 P-NP challenge, 351–352,
 415–417
 pre-publication review by
 U.S., 306–307
 pros/cons of control,
 309–310
 protecting aircraft signals,
 315
 public key encryption,
 308–309, 310,
 349–350, 451, 453. *See*
also R.S.A. system
 signing on to computers,
 315
 tighter security rules,
 308–311
 zero-knowledge proof and,
 312–315, 316–318
 Cryptos package, 336
 Currents, finding order in,
 184–187
- D**
 Data Encryption Standard
 (D.E.S.), 328–330,
 331–333. *See also*
 Cryptography
 Daubechies, Ingrid, 388, 389
 Davida, George I., 309, 310, 318
 Davies, Paul, 7, 8
 Deavours, Cipher, 331, 333
 Definitions of mathematics. *See*
 What mathematics is
 Dehaene, Stanislas, 4–6, 8
 Della-Latta, Phyllis, 296–297
 Deolalikar, Vinay, 415–416, 417
 Derman, Emanuel, 90
 Dertouzos, Michael, 310, 311
 D.E.S.. *See* Data Encryption
 Standard (D.E.S.)
 Diaconis, Persi
 on “bootstrap” method,
 31–32
 on clusters, 279
 on coincidences, 283, 288
 explaining coincidences,
 35–39
 on Monty Hall Problem,
 45–46, 47
 seeing patterns in random
 data, 55–56
 solving shuffling problem,
 73–76, 267–268
 Diamond, Fred, 158, 161, 162,
 163
 Diffie, Whitfield, 304, 308,
 332, 333, 335–336,
 339, 452–453
 Disease clusters, 36, 278–280,
 292
 DNA. *See* Genetics
 Donaldson, Simon, 11, 12
 Doorley, John, 412
 Dreitzer, Howard, 74
*The Drunkard’s Walk: How
 Randomness Rules Our
 Lives* (Mlodinow), 93
 Dudley, Underwood, 459, 461,
 462
 Dyson, Freeman, 194, 443
- E**
 Eckert, J. Presper, 361, 396,
 398
 Eckmann, Jean-Pierre, 17–18
 Economy and economics. *See*
also Stock market,
 chaos ruling
 games theory applied to
 business problems,
 169–172
 Mandelbrot concepts
 affecting, 232, 233–234
 modeling risk without
 human factor, 88–91
 pre-computer input-output
 model, 64–66
 program figuring out
 market, 107–109
 uncertainty of forecasting,
 274–277
 Edge Foundation, 5
 Edvac, 358
 Edwards, Harold M., 146, 147
 E8, 190–191
 Efron, Bradley, 29, 30–32, 36,
 283, 284–285
 Einstein, Albert
 quantum mechanics, 429
 quotes, 4, 70
 theory of relativity, 115,
 116–117, 122, 429
 unifying theories of, 115–118
 Eisenberg, Anne
 article by, 403–405
 biography, 463
 Encryption. *See* Cryptography;
 National Security
 Agency (N.S.A.)
 ENIAC, 357, 358–359, 361,
 396, 398–399
 Erdos number, 421
 Erdos, Paul, xv–xvi, 93, 198,
 420–422
 Evans, Donald L., 51
 Evans, John B., 108
 Extinctions, mass, 67–69
- F**
 Factorial, 52, permutations, 73
 Factoring
 100-digit number, 319–323
 129-digit number, 27–28
 155-digit number into three
 prime factors, 324–327
 155-digit number into two
 prime factors, 343–344
 about: overview of, xiv–xv
 difficulty of, 268–269
 protecting computer data
 and, 407
 Fajtlowicz, Siemion, 13–15
 Falk, Ruma, 291–292
 Faltings, Gerd, 9, 12, 142, 159,
 162
 Farmer, J. Doynce, 212, 219, 230
 Faure, Lt. Gen. Lincoln, 309
 Feder, Stanley, 84, 85, 86
 Fefferman, Charles, 423, 425
 Feigenbaum, Mitchell
 background and education,
 209, 213–215
 Chaos ’87 presentation, 241
 as chaos theory midwife,
 208
 computer use, 216–218
 demeanor and work ethic,
 213–214, 218
 developing chaos theory,
 210–213
 discovering first universal
 constant, 215
 intuitive approach, 216–217
 period doubling and,
 212–213, 215–216, 220
 “pictures” of inspiration, 215
 pondering chaos in nature,
 208
 reputation, 214
 scaling inspiration, 216,
 221–222

INDEX

- vision of chaos applications, 221–222
- Feige, Uriel, 312
- Ferguson, William, 342
- Fermat's Last Theorem, 139–163. *See also*
 - Wiles, Andrew
- about: overview of, 113–114, 145
- bridging gap in, 157, 158–163
- checking proof, 155–156
- coming up short on solving, 141, 142–144
- confidence from solving, 153–154
- crank mail on, 460
- delineated, 139, 146, 150, 157
- development of, 150–151
- Flach method and, 160, 161
- flaw in proof, 155–156
- haunting words regarding, 139
- impending solution, 139–140
- jealousy, gossip and, 156
- as “lost gold mine,” 139–140
- luring cranks, 146–147
- marginal proof, 143–144
- Miyaoka and, 139, 140, 141, 142, 144
- prized offered for solution, 147
- published works, 219
- Q.E.D. (or not), 149, 157
- Ribet and, 144, 145–146, 147, 148–149, 152, 156, 160, 446
- solving of, 145–149, 151–154, 155, 158–159, 418–419, 444–448
- Taniyama conjecture and, 147–148, 152–153, 157, 158, 162–163, 445–446
- tortuous path to proof, 147–148
- translation, 152–153
- Ferrenberg, Alan M., 270, 271, 272, 273
- Fiat, Amos, 312
- Fish
 - population, chaos example, 212–213
 - schooling of, 256–260
- Fisher, Michael, 229, 245
- Flach method (Matthias Flach), 160, 161
- Flint, Peter B.
 - article by, 456–457
 - biography, 463
- Flocking and schooling, 256–260
- Flow patterns, finding order in
 - currents, 184–187
- Fluid math, 243–245
- Ford, Joseph, 209, 219, 221
- Forecasting, uncertainty of, 274–277
- Four-color problem and proof, xi, 135, 136
- Fourier analysis, 191, 388, 389
- 42d Street, closing, 48–50
- Fractals. *See also* Mandelbrot, Benoit
 - complexity of nature and, 224
 - continuum, branching and, 227
 - describing how things cluster in time/space, 226
 - examples, 298–299
 - helping understand chaos, 225
 - impact on geometry and world, 223–224, 225–226, 232–234, 298, 300
 - infinite self-embeddedness and, 228
 - key to, 227–228
 - in nature, 68
 - new symmetry from, 225–226
 - “noise” in transmission lines and, 226
 - pervasiveness of, 224
 - revealing unity, 227
 - as shapes with fractional dimensions, 227–228
 - term origin, 224
- Freedman, David, 52, 280
- Freedman, Michael, 9, 10, 11, 12, 121, 130
- Frey, Gerhard, 147, 153, 445–446
- Friedman, Harvey, 265–266
- Friedman, Jerome H., 29, 30, 31
- Frye, Roger, 143
- Fry, John, 194
- G**
 - Galil, Zvi, 316, 318
 - Gallagher, Bobbie and Alanna, 278
 - Gall, Bob, 53
 - Games
 - Cardano's method and, 92–93
 - Monty Hall Problem, 43–47, 93
 - playing the odds, 92–94
 - Game theory
 - applied to business problems, 169–172
 - political predictions and, 77–79, 81
 - selfishness and, 49–50
 - Gang Tian, 123
 - Garcia, A., 128–129
 - Gardner, Martin, 44, 45, 142–143, 154, 452
 - Garey, Michael, 199
 - Gaussian elimination, 322
 - Gauss, Karl Friedrich, 193, 384, 458
 - Gaynor, Kevin, 81
 - Genetics
 - deciphering DNA, 345–348
 - DNA as computer, 450, 454–455
 - longevity/traits odds, 102–105
 - theory of knots and DNA, 175–178, 179
 - Geometry, classical, nature's complexity and, 224
 - Geometry, fractals and. *See* Fractals; Mandelbrot, Benoit
 - Gessen, Masha, 131, 132
 - Gleick, James, article topics
 - chaos, 208–222, 239–242, 246–255
 - computer as mathematics tool, 16–18
 - cryptography, 312–315
 - Fermat's Last Theorem, 139–144, 150–154
 - flocking and schooling, 256–260
 - fluid math, 243–245
 - fractals, 224–228, 230, 232–234, 298–300
 - heavier objects rising to top, 40–42

INDEX

- Gleick, James, article topics
 (continued)
 Mandelbrot and geometry,
 223–234
 Ramanujan, Srinivasa,
 438–443
 secrets of knots, 175–180
 Shannon, Claude, 436–437
 snowflakes and
 randomness, 235–238
 solitons and
 superconductors,
 261–264
 true randomness, 265–269
 truth and beauty of
 mathematics, 9–12
 Gleick, James, biography, 463
 Glimm, James, 241
 Glotzer, Sharon C., 182, 183
 Gödel, Kurt
 “axiom of choice” and, 168
 continuum hypothesis and,
 167
 eulogistic perspective,
 456–457
 showing incompleteness/
 insolvability/
 undecidability, 117, 118,
 137, 143–144, 154, 452,
 456–457
 Gödel’s Theorem, 456
 Goertzel, Ben, 107, 108, 109
 Goldbach’s conjecture
 (Christian Goldbach),
 137–138, 460
 Goldwasser, Shafi, 268, 314
 Gomory, Ralph E., 227
 Gott, J. Richard, 277
 Gowers, Timothy, 417
 Graham, Ronald L.
 on Fermat’s Last Theorem,
 139, 142
 on John Conway, 430
 on Khachiyan’s linear
 programming ideas,
 409
 lesson in problem difficulty,
 408
 on Paul Erdos, 420,
 421–422
 on random-number
 generators, 272
 on RSA System, 320
 on shortest path to connect
 set of points, 198, 199
 Green, Donald, 85
 Greene, Ben, 425
 Greene, Robert, 122, 123
 Greenspan, Alan, 107, 108
 Gumbel, E. J., 170, 172
 Gurney, Ian, 293–294, 295
H
 Haken, Wolfgang, 25, 136
 Hales, Thomas C., 181
 Haller, George, 186, 187
 Hall, Monty (Problem), 43–47,
 93
 Hamilton, Richard, 122, 124,
 133, 134
 Hamner, William M., 259, 260
 Happy Birthday puzzle, 95–101.
 See also Birthdays
 Harary, Frank, 25
 Hardy, Godfrey Harold, 192,
 440–442, 443, 458
 Hasslacher, Brosi, 244
 Health care debate, mining
 patient records,
 410–414
 Heavier objects rising to top,
 40–42
 Heisenberg’s Uncertainty
 Principle, 458
 Hellman, Martin E.
 encryption security issues,
 309, 311, 330, 332
 N.S.A. harassment
 allegation and, 304,
 305
 on N.S.A. review
 cooperation, 307
 R.S.A. system and,
 308–309, 452–453
 secrecy protest, 339
 Heppner, Frank, 257, 259
 Hersh, Reuben, 3, 7, 460, 461
 Hillman, Alan, L., 413, 414
 Hinton, Geoffrey, 404
 H.I.V., 94, 287, 294
 Hoffman, David A., 16, 17
 Hoffman, Jascha
 article by, 131–132
 biography, 463
 Hoffman, Paul
 biography, 463–464
 Foreword by, x–xii
 Holberton, Frances E. “Betty,”
 398–399
 Holzmayer, Tanya, 296
 Hopper, Rear Adm. Grace M.,
 395–397
 Hopper, Thomas, 386
 Housing prices/bubble, 89–90
 Howard, Michael, 112
 Huai-Dong Cao, 123
 Huffman coding, 400–401
 Hurwicz, Leonid, 170, 172
 Hwang, Frank, 198, 199
I
 Images, storing efficiently,
 385–389, 400–401
 Infinite self-embeddedness, 228
 Inman, (Vice) Adm. Bobby R.,
 309, 318
Innumeracy (Paulos), 282
 Insurance, 62–63
 Insurance companies, mining
 patient records and,
 410–414
 Iran, getting nuclear bomb,
 77–87
 I.R.S., sniffing out tax cheats,
 110–112
J
 Jacquard, Joseph Marie, 360
 Janus supercomputer, 390–394
 Jefferson, David, 450
 Jefferson, Thomas, 99, 289
 Jim twins, 102–103
 Johnson, David (of Bell
 Laboratories), 199
 Johnson, George
 articles by, 3–8, 92–94,
 137–138, 390–394,
 458–462
 biography, 464
 Johnston, David Cay
 article by, 110–112
 biography, 464
 Joint pain (arthritis), weather
 and, 54–57, 291
 Jones, Vaughan F.R., 177
K
 Kadanoff, Leo, 229, 245
 Kahn, David, 331
 Kaliski, Burt, 343
 Kaplan, Edgar, 74
 Kaplan, James L., 250
 Karp, Richard, 382, 384
 Kassirer, Jerome P., 412
 Katz, Nicholas, 147–148, 159,
 447
 Kelley, Robert F., 83
 Kelly, Frank P., 48, 49

INDEX

- Kennedy/Lincoln deaths,
294–295
- Khachiyan, L.G., 406, 407, 409
- Kinderlehrer, David, 189
- Kleiman, Kathryn, 399
- Kleitman, Daniel, 24
- Knots, theory and secrets of,
175–180
- Knuth, Donald E., 398
- Koch curve, 228
- Kochen, Simon, 153, 444–445,
447, 448
- Kocher, Paul, 350
- Kolata, Gina, article topics.
See also Kolata, Gina,
computer-related topics
- Adleman, Leonard,
449–455
- breaking encryption
standard, 331–333
- closing of 42d Street, 48–50
- coincidences, 35–39
- Conway, John H., 430–435
- disease clusters, 278–280
- Erds, Paul, 420–422
- factoring 155-digit number
into three prime factors,
324–327
- Fermat's Last Theorem,
145–149, 155–156, 157,
158–163
- genetic roulette odds,
102–105
- health care debate, 410–414
- Riemann hypothesis,
196–197
- shortcut for checking long
proofs, 381–384
- shortest path to connect set
of points, 198–199
- shuffling cards, 73–76
- storing images more
efficiently, 385–389
- 2000 election counts, 106
- weather/arthritis pain
relationship, 54–57
- why some numbers are only
guesses, 51–53
- Wiles, Andrew, 444–448
- Kolata, Gina, biography, 464
- Kolata, Gina, computer-related
topics
- computer-aided proofs,
24–26
- computer reasoning power,
19–23
- conjectures, 13–15
- factoring 129-digit number,
27–28
- uncertainty and computers,
29–32
- Korshunov, Victor, 295–296
- Kronecker, Leopold, 4
- L**
- Lagarias, Jeffrey C., 182
- Lakoff, George, 4, 6–7
- Landau, D. P., 270
- Landauer, Rolf, 393, 394
- Lander, Eric S., 346, 347, 348
- Langer, James S., 235, 236, 237
- Langford, Ian, 296
- Langlands program, 158,
162–163, 446
- Lansing, Sherry, 93–94
- Laphorne, Richard, 83, 84
- Laurence, William L.
articles by, 115–118, 135
biography, 464
- Lee, Daniel, 403, 404, 405
- Lee, T. D., 262
- Lehmann, Erich, 35
- Lekien, Francois, 186
- Lempel-Ziv compression, 400,
401
- Lenstra, Argen, 28, 319, 321,
324, 325, 326, 344
- Lenstra, Hendrik, 326
- Leontief, Wassily, 64–66
- Let's Make a Deal*. See Monty
Hall Problem
- Levi-Civita, Tullio, 116, 117
- Levine, Herbert, 235, 236
- Levin, Leonid, 266
- Lewis, Jim, 102–103
- Lieberman, Henry L.
article by Louis Robinson
and, 360–380
biography, 464
- The Limits of Mathematics*
(Chaitin), 4
- Lincoln/Kennedy deaths,
294–295
- Lindemann, Ferdinand,
460–461
- Lindsey, Richard R., 90–91
- Lissner, Will
articles by, 169–172,
358–359
biography, 465
- Little, C. N., 177
- Lo, Andrew W., 88, 91
- Lockshin, Michael, 56
- Lohr, Steve
articles by, 88–91, 398–399
biography, 465
- Lorenz, Edward N., xiv, 211
- Lottery, draft, randomness and,
266–267, 268
- Lottery, state, winning twice,
37–38
- M**
- MacPherson, Robert D., 188,
189
- Magicians, 75–76, 101. See also
Diaconis, Persi
- Mallat, Stéphane, 388–389
- Manasse, Mark S., 319, 320,
321–322, 326
- Mandelbrot, Benoit, 223–234,
298–300. See also
Fractals
- analyzing "noise" in
transmission lines, 226
- approaches to people in
various disciplines,
231–232
- attitude toward
establishment, 231
- background and education,
224–225, 231, 298
- "Clouds are not spheres . . ."
statement, 224, 298
- colleagues' perspective, 225,
229, 230
- consistent message of, 299
- ego, credit and, 223, 225,
229–230
- eulogistic perspective,
298–300
- on extreme events, 254
- impact on economics, 232
- impact on geometry,
223–224, 225–226
- on intuition, 229
- "looking in trash cans of
science," 228, 299
- perspective and outlook,
223, 225, 230–232,
233–234
- politics affecting style,
230–231
- self-similarity and,
226–227, 229, 231, 232
- on stock price
characteristics, 251
- Manrubia, Susanna C., 68

INDEX

- Market. See Economy and economics
- Markoff, John
 articles by, 328–330,
 334–337, 338–342,
 349–350, 351–352,
 395–397, 415–417
 biography, 465
- Marsaglia, George, 269
- Marsden, Jerrold E., 185, 187
- Mass extinctions, 67–69
- Mauchly, John W., 361, 396,
 398
- May, Robert M., 212, 213, 254
- Mazur, Barry, 144, 146, 151,
 156, 447
- McConnell, Rear Adm. John
 M., 337
- McCune, William, 19, 20,
 22–23
- McDermott, Rose, 84
- McGovern, George, 67
- McKay, Brendan, 24–25
- Medical records, mining,
 410–414
- Merkle, Ralph, 308, 339
- Merold, Robert, 410
- Mesirov, Jill P., 347
- Metal, shape-shifting, 188–189
- Meyer, David A., 276
- Meyer, Joseph A., 305
- Meyer, Yves, 388
- Micali, Silvio, 268, 269, 312,
 314
- Milnor, John, 11
- Mining patient records,
 410–414
- The (Mis)behavior of Markets*
 (Mandelbrot), 299
- Miyaoka, Yoichi, 139, 140, 141,
 142, 144
- Mizuuchi, Kiyoshi, 175
- Mlodinow, Leonard, 92–94
- Modeling
 game theory and political
 projections, 77–87
 risk, with human factor left
 out, 88–91
- Monroe, James, 99
- Montgomery, Hugh, 194, 195
- Monty Hall Problem, 43–47,
 93
- Moons and asteroids, chaos
 and, 239–242
- Morgan, Frank, 173, 174
- Morgan, John, 120, 121, 123
- Morgenstern, Oskar, 169, 170,
 171, 172
- Morlet, Jean, 387–388
- Morris, Carl, 414
- Mosteller, Frederick, 29, 35–37,
 38, 39
- Mostow, Steven, 296
- Motwani, Rajeev, 381, 382
- Mumford, David B., 225, 229
- Mutalik, Pradeep
 article by, 95–101
 biography, 465
- Mutz, Diana C., 106
- Myhrvold, Nathan P., 334
- My Life as a Quant—
 Reflections on Physics
 and Finance* (Derman),
 90–91
- ## N
- National Security Agency
 (N.S.A.)
 breaking encryption
 standard and, 331–333
 Clipper/Tessera technology,
 339–342
 code keys control
 controversy and,
 334–337
 encroaching onto civilian
 turf, 338–342
 factoring 100-digit number
 and, 322
 harassment alleged over
 research, 303–305
 as No Such Agency, 317
 reviewing pre-publication
 research, 306–307
 R.S.A. system and,
 453–454
 suppressing zero-knowledge
 proof, 316–318
 tighter security rules,
 308–311
- Neumann, Peter, 52
- Newton, Isaac, 191, 275–276
- Nguyen, Kathy, 294, 295
- Nguyen, Set Van, 293, 294,
 295
- Nondeterministic Polynomial
 Complete Problem (N-P
 Complete), 304
- N.S.A.. See National Security
 Agency (N.S.A.)
- The Number Sense: How
 the Mind Creates*
- Mathematics*
 (Dehaene), 3–6
- Núñez, Rafael E., 4, 6–7
- ## O
- Odds, playing, 92–94
- Odlyzko, Andrew M., 196, 321,
 323, 324
- Okounkov, Andrei, 428, 429
- Olsen, Kenneth H., 395
- Organski, A.F.K., 82
- Osmundsen, John A.
 article by, 164–168
 biography, 465
- Overbye, Dennis
 articles by, 119–124,
 125–130, 133–134
 biography, 465
- ## P
- Packard, Norman H., 244
- Packing tetrahedrons, 181–183
- Pasechnik, Vladimir, 281,
 292–293, 294, 296
- Paths, shortest between set of
 points, 198–199
- Patterns
 algorithm recognizing,
 403–405
 brains and, 260
 chaos and, 210, 213,
 215–216, 217, 218–219,
 220
 deceptive nature of, 260
 flocking, schooling and,
 256–260
 flow, finding order in
 currents, 184–187
 not as they appear,
 282–283. *See also*
 Coincidences
 in random data, 55–56
- Patterson, Nick, 345–348
- Paulos, John Allen
 biography, 465
 on birthday matches,
 285–286
 on coincidences, 282,
 288–289
 on crank math-related mail,
 260
Innumeracy of, 282
 “Metric Mania” article by,
 70–72
- Pazer, Lisa S., 107, 108, 109
- Peacock, Thomas, 185–186

- Pereira, Fernando C. N., 404, 405
- Perelman, Grigori "Grisha."
See also Pointcaré conjecture
 awarded Fields Medal, 133
 background and education, 122–123, 131–132
 beautiful mind of, 131–132
 declining \$1 million prize, 133–134, 415, 428–429
 elusiveness of, 119–120, 123, 131–132, 133–134
 physical description, 123, 131
 solving Pointcaré conjecture, 119–120, 123–124
 William Thurston and, 120, 121, 122, 126, 133
- Perfect Rigor* (Gessen), 131, 132
- Perl, Martin L., 31
- Perpetual motion, 262–263
- Peto, Richard, 411
- Pi, 7, 433–434, 443, 461
- Pierce, Charles P., 104
- Pines, David, 247, 253, 261
- Planets, motion of, chaos and, 202–203. *See also* Moons and asteroids
- Plateau, Joseph A. F., 173
 Plateau's problem, 173–174
 P-NP challenge, 351–352, 415–417
- Pointcaré conjecture
 about: overview of, 114
 description of, 120–121
 difficulty of proving, 121
 efforts at proving, 121–124
 examples, 127–128
 follow-up proof, 123
 importance of, 126–127
 importance to topology, 120–122, 129–130
 multiple dimensions and, 121, 125–126, 128
 nature of space and, 119, 120–122, 128
 paradoxes and, 128–129
 Perelman solving, 119–120, 123–124
 posed, 120
 questions and answers, 125–130
 rabbit as sphere, 120, 125
 Ricci flow and, 122, 126, 127, 429
- Richard Hamilton and, 122, 124, 133, 134
- Poker
 playing the odds, 92–94
 shuffling cards and, 33, 35, 73–76, 267–268
 theory of, applied to business, 169–172
- Political world. *See also* Cryptography; National Security Agency (N.S.A.)
 C.I.A. predictions, 84
 game theory and political projections, 77–87
 predicting how leaders behave, 79–80
 predicting nuclear capabilities of Iran, 77–79, 87
 sniffing out tax cheats, 110–112
 2000 election counts, 106
- Polyakov, Aleksandr, 10–11
- Polynomials, knot theory and, 177–178, 180
- Potts, Wayne K., 257, 258, 259
- Powders, mixing, 42
- Prime numbers
 factoring and. *See* Factoring
 Goldbach's conjecture and, 137–138
 Riemann hypothesis and, 192–195, 196–197
 Tao's work on, 425
 twin, xi, 425
- Prinz, Friedrich, 40, 41
- Prize money
 Perelman declining \$1 million, 133–134, 415, 428–429
 P-NP challenge and controversy, 351, 415–417
- Problems, famous. *See also* Fermat's Last Theorem; Pointcaré conjecture
 about: overview of, 113–114
 classic Greek problems, 460–461
 crank solutions and, 458–462
 finding order in currents, 184–187
 four-color problem and proof, xi, 135, 136
- Goldbach's conjecture, 137–138
 packing tetrahedrons, 181–183
 perfect symmetry, 190–191
 Plateau's problem, 173–174
 Riemann hypothesis, 160, 192–195, 196–197
 set theory proof, 164–168
 shape-shifting bubbles and metal, 188–189
 shortest path to connect set of points, 198–199
 theory of games applied to business, 169–172
 theory of knots, 175–180
 3-D curve surface area bounded by curve, 173–174
 unifying relativity and quantum mechanics, 115–118
- Proofs, checking, 381–384
- Public key encryption, 308–309, 310, 349–350, 451, 453

Q

- Quarters, rising to top, 42
- Que, Benito, 281, 286–287, 294
- Quesnay, François, 65

R

- Radziszowski, Stanislaw P., 24–25
- Rajan, Raghuram G., 89
- Ramanujan, Srinivasa, 418, 438–443, 458–459, 460, 462
- Ramsey, James, 246, 250, 252
- Randomness. *See also* Coincidences
 about: overview of, 200–201
 catch-22 of, 272–273
 coin-tossing and, 92, 99, 265
 coin-tossing computers and, 270–273
 playing odds and, 92–94
 playing the odds, 92–94
 shuffling cards and, 33, 35, 73–76, 267–268
 snowflakes and, 235–238
 true, generating, 265–269
- Rattner, Justin, 393
- Raup, David M., 69

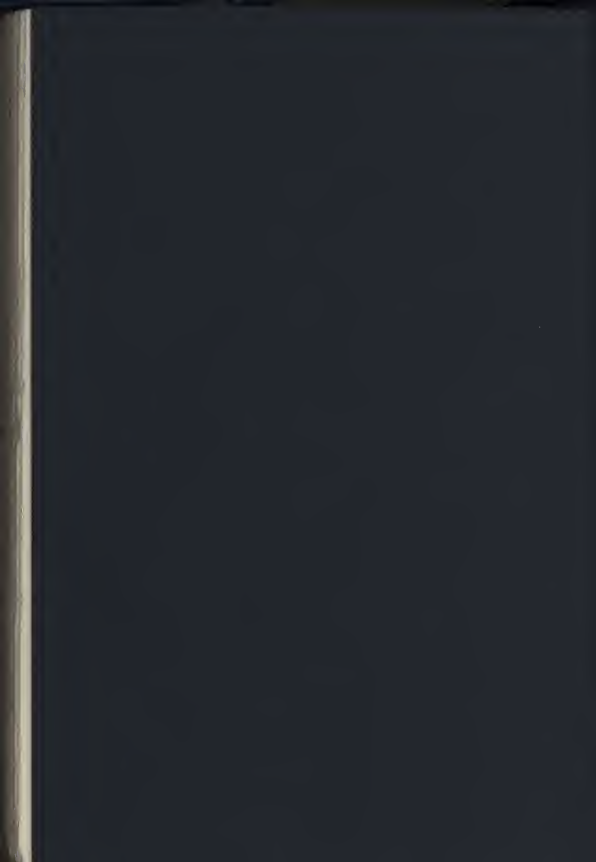
INDEX

- Redelmeier, Donald A., 55, 56
Red Flag over Hong Kong
 (Bueno de Mesquita), 86
- Reed, Jim, 75, 272
- Reeds, James, 75, 272
- Reich, David, 345, 348
- Reichelderfer, Francis, 60
- Reinsch, William, 343
- Resnikoff, Howard L., 385
- Reynolds, Craig W., 256–257, 259
- Ribet, Kenneth, Fermat's Last Theorem and, 144, 145–146, 147, 148–149, 152, 156, 160, 446
- Ricci flow, 122, 126, 127, 429
- Riccio, Lucius, 48, 50
- Riemann geometry, 117
- Riemann, Georg Friedrich Bernhard, 121, 126.
See also Riemann hypothesis
- Riemann hypothesis, 160, 192–195, 196–197
- Riemann's zeta function, 193–194, 195, 196, 197, 458
- Riker, William H., 79
- Rivest, Ronald
 on encryption standard status, 328
 N.S.A. financing and, 307
 R.S.A. system and, 27, 308–309, 343–344, 452–453
 on secrecy order, 318
 secrecy protest, 339
- Robbins, Herbert, 20, 22
- Robins, James, 279, 280, 292, 295
- Robinson, Louis, article by Henry L. Lieberman and, 360–380
- Robinson, Sara
 article by, 343–344
 biography, 465
- Roper, William, 411, 413
- Rosen, Michael, 162
- Roses, Allen, 103–104, 105
- Rota, Gian-Carlo, 432
- Roundell, Harry, 82, 84–85
- R.S.A. system
 about: overview of, 308–309
 acronym meaning, 420
 breaking code, 343–344
 chip production, 454
 code keys control controversy, 334–337
 origins, 308–309, 420, 452–455
 R.S.A. 129, 27–28
- Ruelle, David, 18
- Rushnell, Squire, 289–290, 292
- S**
- Sachs, Robert, 44, 45–46
- Sarnak, Peter, 195
- Schechter, Bruce
 article by, 192–195
 biography, 465
- Schooling and flocking, 256–260
- Schrieffer, Robert, 261–262, 263, 264
- Schwartz, Daniel, 306–307, 311
- Schwartz, Robert, 293, 294
- Self-embeddedness, infinite, 228
- Self-similarity, 68, 226–227, 229, 231, 232
- Set theory proof, 164–168
- Seung, Sebastian, 403, 404, 405
- Severo, Richard
 article by, 306–307
 biography, 466
- Shalett, Sidney
 article by, 58–61
 biography, 466
- Shamir, Adi
 attacking encryption standard, 328–329, 330, 332–333
 on PC chip security, 349–350
 photograph, 349
 R.S.A. system and, 27, 308–309, 343–344, 350, 453
 zero-knowledge proof and, 312–313, 314, 316–318
- Shannon, Claude, 361, 400, 401, 436–437
- Shape-shifting bubbles and metal, 188–189
- Shaw, Robert, 219, 220
- Shimura, Goro, 147
- Shirky, Clay, 416–417
- Shoemaker, Janet, 296
- Shub, Michael, 268
- Shuffling cards, 33, 35, 73–76, 267–268
- Sieveking, Paul, 295
- Silk, Leonard
 article by, 64–66
 biography, 466
- Simmons, Gus, 325–326
- Simon, Col. Leslie E., 358–359
- Simon, Jonathan, 178
- Simonovits, Miki, 420
- Simons, James H., 347
- Simplex algorithm, 408–409
- Simpson, Nichole Brown, 94
- Simpson, O. J., 94
- Sipser, Michael, 381
- Sloane, Neil, 432, 434
- Smale, Stephen, 16–17, 121, 206–207
- Smart cards, 312–313, 314
- Smith, O.C., 297
- Smullyan, Raymond M., 164
- Snowflakes, 235–238
- Soap bubbles, 173–174, 236
- Solé, Ricard V., 68
- Solitons, 261–262, 263–264
- Sparrow, Malcolm, 112
- Spencer, Joel H., 420, 421
- Springer, Jim, 102–103
- Srolovitz, David J., 188, 189
- Statistics. *See also*
 Coincidences;
 Randomness
 about: overview of, 33–34
 “bootstrap” technology, 30–31
 census-related problems, 51–52, 53, 357
 computers addressing uncertainty, 29–32
 counting and aggregating, 70–72
 heavier objects rising to top, 40–42
 insurance and, 62–63
 mass extinctions, 67–69
 Monty Hall Problem, 43–47, 93
 nuclear capability of Iran (prediction), 77–87
 patterns in random data, 55–56
 pre-computer economy input-output model, 64–66
 sniffing out tax cheats, 110–112

- traffic flow and closing 42d
 - Street, 48–50
 - voting-related problems, 30, 51, 52, 53, 72, 79, 106
 - weather forecasting and.
 - See Weather
 - why some numbers are only guesses, 51–53
 - Stewart, Ian, 264, 459, 461–462
 - Stites, Janet
 - article by, 107–109
 - biography, 466
 - Stock market, chaos ruling, 246–255
 - about: overview of, 246–248
 - Black Monday (Oct. 19, 1987) and, 248–250, 253
 - chaos defined, 247
 - character of price changes and, 250–251
 - choosing right/wrong way to look at market, 255
 - evidence of, 246–247
 - extreme events and, 247–248, 254
 - global instability and, 248–250
 - program trading and, 249–250
 - random-walk approach and, 253–254
 - unpredictable forces and, 251–253
 - Strandburg, Katherine J., 40, 42
 - Strange attractors, 218–219
 - Straus, Ernst, 420
 - Sudan, Madhu, 381
 - Sullivan, Walter
 - article by, 308–311
 - biography, 466
 - Supercomputers, 190, 243, 244, 321, 390–394
 - Superconductors, 261–264
 - Sussman, Hector J., 206
 - Swendsen, Robert H., 40
 - Symmetry, perfect, 190–191
- T**
- Tait, Guthrie, 177
 - Taniyama conjecture (Yutaka Taniyama), 147–148, 152–153, 157, 158, 162–163, 445–446
 - Tao, Terence, 423–427, 428, 429
 - Tax cheats, finding, 110–112
 - Taylor, Richard, 160–161, 162, 163
 - Tenenbaum, Joshua B., 289
 - Tenner, Edward, 53
 - Tessera/Clipper technology, 339–342
 - Tetrahedrons, packing, 181–183
 - Theory of Games and Economic Behavior* (von Neumann), 169
 - The Theory of Political Coalitions* (Riker), 79
 - Thistlethwaite, Morwen B., 176
 - Thompson, Clive
 - article by, 77–87
 - biography, 466
 - Thom, René, 69, 205, 207, 276–277
 - 3-D curve surface area bounded by curve, 173–174
 - Thurston, William, 120, 121, 126, 133
 - Tibshirani, Robert J., 285
 - Tierney, John
 - article by, 43–47
 - biography, 466
 - Tighter security rules, 308–311
 - Tinkertoy analogy, 387–388
 - Toffoli, Tommaso, 244
 - Topology
 - catastrophe theory and, 69, 205
 - defined, 120
 - knots and, 175–180
 - Poincaré conjecture and.
 - See Perelman, Grigori
 - "Grisha"; Poincaré conjecture
 - Torquato, Salvatore, 181, 182, 183
 - Traffic flow, 48–50, 260
 - Traveling salesman problem, 351, 352, 353, 407
 - Turing, Alan, 137, 138, 346–347, 361
 - Tversky, Amos, 54–57, 290–291
 - Twain, Mark, 61, 173
 - 2000 Election counting, 106
- U**
- Ulam, Stanislaw M., 271
 - Uncertainty
 - computers and, 29–32
 - of forecasting, 274–277
 - Heisenberg's Uncertainty Principle, 458
 - inherent, in proofs, 383–384
 - Unifying theories, 115–118
 - Langlands program, 158, 162–163, 446
 - "The Unreasonable Effectiveness of Mathematics in the Natural Sciences" (Wigner), 1
- V**
- Valiant, Leslie G., 12
 - Vardi, Moshe, 352, 416
 - Vazirani, Umesh, 382
 - Venkataraman, Bina
 - article by, 184–187
 - biography, 466
 - Virus, computer, 449, 454
 - Von Neumann, John
 - biographical sketch, 169, 361
 - computer development and, 358–359, 361
 - on computers, 272
 - fluid-simulation models and, 244
 - on Kurt Gödel, 456
 - mathematical theory of games/poker, 169–172
 - weather-forecasting machine, 58–61
 - Vos Savant, Marilyn, 43–44, 45, 46, 47
 - Voss, Richard F., 228, 234
 - Voting-related problems, 30, 51, 52, 53, 72, 79, 106
- W**
- Wainer, Howard, 106
 - Walker, Stephen, 341
 - Walt, Stephen, 85–86
 - Wasson, John, 413
 - Waves, finding order in currents, 184–187
 - Wayner, Peter
 - article by, 400–402
 - biography, 466
 - Weather
 - arthritis pain and, 54–57, 291
 - early forecasting machine, 58–61

INDEX

- Weather (*continued*)
 satellites, storing data for,
 386, 389
 Webmind, 107–109
 Weinberg, Steven, 276
 Weisner, Louis, 171, 172
 Welsh, H. Gilbert, 412
 Werner, Wendelin, 428, 429
 Wetherill, George, 241, 242
What Is Mathematics Really?
 (Hersh), 3
 What mathematics is
 about: overview of, 1–2
 perspectives on practicality,
 9–12
 Platonist views and, 4, 6,
 7–8
 truth, beauty, and
 practicality, 9–12
 useful invention or absolute
 truth, 3–8
*When God Winks: How the
 Power of Coincidence
 Guides Your Life*
 (Rushnell), 290
 Wickerhauser, Victor, 385–386,
 389
 Wiener, Norbert, 200,
 202–203, 261
 Wigner, Eugene, 1, 2
 Wiles, Andrew, 444–448
 age considerations, 151–152
 background and education,
 445
 bridging gap in proof, 157,
 158–163
 demeanor of, 148
 Fields Medal eligibility, 151
 flaw in Fermat proof,
 155–156
 jealousy and gossip about,
 156
 presenting Fermat solution,
 148
 Riemann hypothesis and,
 192
 solving Fermat's Last
 Theorem, 145–149,
 151–154, 155, 158–159,
 418–419, 444–448
 Taniyama conjecture and,
 147–148, 152–153, 157,
 158, 162–163, 445–446
 translation of Fermat
 solution, 152–153
 Wiley, Don C., 281, 287–288,
 294, 295, 297
 Willen, Paul S., 90
 Williams, Joseph
 article by, 173–174
 biography, 466
 Wilson, Kenneth G., 210, 216,
 229
 Winfree, Arthur T., 179
 Wisdom, Jack, 239, 241, 242
 Witten, Edward, 10, 126–127
 Wolfram, Stephen, 244, 269
 Wong, Joanna, 270, 271
 Wos, Larry, 19, 20–22, 23
 Wynn-Williams, David, 296
- ## X
- Xi-Ping Zhu, 123
- ## Y
- Yang Jiao, 183
 Yannakakis, Mihalis, 382
 Yao, Andrew, 268
 Yau, Shing-Tung, 119, 130
 Yetter, David, 178
- ## Z
- Zagier, Don, 141
 Zahler, Raphael S., 206
 Zeeman, E. Christopher,
 205–207
 Zero-knowledge proof, 312–315
 Zeta function. *See* Riemann
 hypothesis
 Zworykin, Vladimir Kosma,
 weather machine and,
 58–61



- "The Odds of That" by Lisa Belkin: "How surprising is it . . . that two 70-year-old men in the same town should die within two hours of each other? Certainly not common, but not unimaginable. But the fact that they were brothers would seem to make the odds more astronomical. This, however, is a superfluous fact. What is significant in their case is that two older men were riding bicycles along a busy highway in a snowstorm, which greatly increases the probability that they would be hit by trucks." —August 11, 2002

- "Can Game Theory Predict When Iran Will Get the Bomb?" by Clive Thompson: "Bueno de Mesquita's most regular client by far has been the C.I.A. He says he has performed more than 1,200 predictions for the agency, tackling questions like 'How fully will France participate in the Strategic Defense Initiative?' and 'What policy will Beijing adopt toward Taiwan's role in the Asian Development Bank?' In 1987, Stanley Feder, a research political scientist for the C.I.A., published a report analyzing forecasts that Bueno de Mesquita's firm did of political events in 27 countries; he found the success rate of its predictions was the same as the C.I.A.'s own analysts, only more precise." —August 12, 2009

GINA KOLATA reports on science and medicine for *The New York Times*. She is also a frequent lecturer, a two-time Pulitzer Prize finalist, and the author of several books including *Rethinking Flun: The New Science of Weight Loss and the Myths and Realities of Dieting* (2007), which was a finalist for the Quill book awards, and *Flu: The Story of the Great Influenza Pandemic of 1918 and the Search for the Virus that Caused It* (1999).

Top math writing from the archives of **The New York Times**

How many times do you have to shuffle playing cards to perfectly mix the deck? Why are snowflakes symmetrical and why are they all different? How was the first computer virus born? The answers to these questions and many more can be found in *The New York Times Book of Mathematics*. Math and science enthusiasts alike will be engaged by everything from startling findings to intriguing insights in 110 articles, including these:

"Beyond Manly Hall's Doors: Puzzle, Debate and Answer"

—John Conway

"Ask Science: Pappetero's Conjecture"

—John Tukey

"Mathematical Theory of Poker Is Applied to Business Problems"

—Will Livinger

"Experts Debate the Prediction of Disasters"

—Makhlouf W. Browne

"Predicting Disease Clusters: Easier to Spot Than Prove"

—Gina Kolata

"Sufficiently Diverse Math Tool to Break a Protected Code"

—John Markoff

"Can't Conquer Virtually Conquer Space and Time"

—George Johnson

"Highest Honor in Mathematics Is Refused"

—Kenneth Chang

ISBN 978-1-4027-9322-6



9 781402 793226

Printed in the United States of America